平成１２年度・セキュリティ研究部会　報告書

セキュリティポリシー研究グループ

「BS7799と企業の情報セキュリティ管理」

セキュリティ技術研究グループ

「ネットワークセキュリティ技術の実践的研究」

平成 13 年 3 月

社団法人　日本情報システム・ユーザー協会

巻頭言

20 世紀最後の年にあたる 2000 年は、インターネットの普及により、全世界のあらゆる

場所と、短時間に、簡単に、しかも極めて低廉なコストで情報交換が可能になっただけではなく、インターネットを基盤とするアプリケーションの発展で、個人や企業間のコンピュータとコンピュータネットワークの利用、いわゆる IT 技術の利用が飛躍的な発展をとげた年であった。

しかし、この発展の基盤を支えるインターネットテクノロジーは、本来の成り立ちからみてセキュリティについて脆弱性を内在している技術であり、使い勝手の良さの追求が先行し、セキュリティ対策については後追いで整備が進んでいる傾向は否めない。

公開鍵暗号方式による個人認証技術や SSL、VPN といった暗号化通信方式など、信頼性の高い通信技術を用いた電子商取引が始まっているが、企業全般への普及にはまだまだ多くの課題を残している。

しかも、こうした電子商取引の本格化は、単に企業におけるネットワークセキュリティの技術的側面にとどまらず、従来からの企業活動の枠組みを根こそぎ変革し、産業全体をも大きく変える可能性を秘めている。企業全体のこれまでの情報セキュリティ対策を基本から考え直し、再構築を指向する時期が到来したと言っても過言ではない。

こうしたことから、ユーザー協会では、今日的な研究課題としてネットワークセキュリティを選び、ユーザー企業のメンバーが２つのグループに分かれ、ほぼ 1 年の間、研究を行ってきた。 セキュリティポリシー研究グループのテーマは「BS7799 と企業の情報セキュリティ管理」、セキュリティ技術研究グループが「ネットワークセキュリティ技術の実践的研究」である。

多忙な業務の中、 1 か月に 1 回という限られた会合での活動では十分な結果を出せたとは言い難い。ユーザーの立場に立ったセキュリティ研究ということで、当報告が会員の皆様に少しでも参考になることを願っている。

［目　次］

BS7799と企業の情報セキュリティ管理

ネットワークセキュリティ技術の実践的研究

セキュリティポリシー研究グループ

BS7799と企業の情報セキュリティ管理

はじめに

ここ数年の間にパソコンの価格は１／２から１／３に下がり、パソコンが各企業に大量に導入されている。１人１台の普及率に達した企業も多くなってきた。インターネットをビジネスで利用するのは当たり前となっている。インターネットの技術はイントラネットにも利用され、Web 対応の情報システムが徐々に増えている。

IT を援用して仕事のやり方が紙媒体から電子媒体中心へと変化し、情報の入手・移動が非常に容易に、かつ瞬時に行えるようになった。情報を共有して知的生産性を上げることが日常的になっている。この変化により、一方で企業の重要な情報資産が漏洩したり、故意に改ざんあるいは破壊されるなどのセキュリティ上の脅威が企業活動の大きなリスクとなってきている。情報の価値については「機密情報管理規定」のような上位規定を各社定めているが、理解することと実行することは別であり、電子化された情報資産の価値判断と取り扱いに多くの社員が戸惑っている。

情報システム部門では技術的視点で情報セキュリティ対策を早期に強化すべきであると考えるが、経営者の視点で見れば、リスク評価が不確実なセキュリティ対策の投資よりも株主への利益還元を優先しがちである。経営トップは利益を拡大する IT 投資には積極的であるが、金をかけたからといって実質的なプロフィットがあるわけではない、投資効果がはっきりしない情報セキュリティ対策には消極的になりがちである。情報セキュリティ対策はいくらお金をかけてもリスクはゼロにならないし、お金をかけてリスクを小さくすればするほど投資効果が見えにくくなる性質がある。どの程度のセキュリティ対策をとればよいのか、指標があれば上申する方も意志決定する方も話が通じやすいものである。企業活動の顕著なリスクとして、近年、経営トップの説明責任（株主および地域社会に対して）が問われる事件が増えている。株主代表訴訟では途方もない金額の賠償判決が出たり、雪印集団食中毒事件では会社のイメージダウンが経営に大きなダメージを与えている。経営トップは危機管理の必要性は十分すぎるほど理解している。

情報セキュリティポリシーを策定し、セキュリティマネジメントを始める絶好のチャンス到来である。JUAS の研究部会のメンバーはほとんどが情報システム部門の人であり、技術者の視点で議論をすることが多いが、本年度は弁護士が参加したので、弁護士の視点から経営トップの責任を明確にすることができた。その他、次の企業グループが情報セキュリティの研究をし、議論をした。この報告書が多くの企業に読まれ、情報セキュリティ管理への取り組みが活発化すれば幸いである。

１．これから起案してプロジェクトを起こし、セキュリティポリシーを策定する企業
２．情報システム部門が先行してセキュリティポリシーを策定している企業
３．BS7799 には準拠していないが既にセキュリティポリシーがあり、その遵守･監査をより効果的に行いたい企業

活動経過

第１回　６月　　オリエンテーション
第２回　７月　　研究目標の設定
　　情報セキュリティポリシーに関するガイドラインの概要
　　研究の進め方（内閣安全保障・危機管理室）
第３回　８月　　研究目標の確認　BS 7799-1: 1999，BS　77992:1999　英和対訳版
　　ポリシー策定の取り組み事例紹介
　　BS7799 の疑問点について議論
第４回　９月　　ポリシー策定の先進ユーザー事例紹介
　　警察学論集　第 53 巻第８号／特集・ハイテク犯罪対策の推進
　　法的視点
　　研究部会の進め方
第５回　10 月　　GSX／山崎氏の講演
　　TALISMAN 2000年２月号／企業経営と情報セキュリティ
　　「BS7799に準拠したセキュリティポリシーマネージメント」
　　PPT資料／BS7799
JUASセミナー　　11 月 21、22 日　富 士通／田渕氏
　　IT セキュリティ国際標準（IS／IEC 17799）
　　BS7799 管理項目の事例
第６回　11 月　　BS7799 についての議論
第７回　12 月　　BS7799 のコンセプトの理解を深める議論
第８回　１月　　IBM／大木氏の講演　PPT 資料／ネットワーク社会と情報セキュリティ
　　フリーディスカッション
第９回　２月　　まとめの議論
第 10 回３ 月　　平成 12 年度セキュリティ研究部会報告書

第１章　研究目的・目標

ネットワークの普及、EC の普及、国際標準、認証制度の制定、人の流動化、株主訴訟、政府の指導等の背景があり、企業はセキュリティ対策およびセキュリティポリシーについて真剣に検討していかなければならない状況にある。本年度の研究部会参加企業の要望を最大公約数的に整理し、次の２テーマを選択した。

(1) BS7799 の理解を進めながら各企業にあったポリシー・フレームが設定できることを目指す。
(2) セキュリティ対策を決めたが実施段階で成果が出ない。どう管理（あるいは監査）をしたらよいかについてガイドラインにまとめる。

BS7799 の規定範囲と規定の中身についての理解は、次の資料の理解あるいは講演を聴くことにより達成した。

① JUAS で「BS7799-1:1999,BS7799-2:1999 英和対訳版」日本規格協会発行を購入し、各自理解。
② ７月に内閣安全保障・危機管理室より「情報セキュリティポリシーに関するガイドラインの概要」が公開され、セキュリティポリシー策定のプロセス、ポリシーに規定する範囲、リスク評価法を理解した。
③ 10 月にはグローバルセキュリティエキスパート（株）山崎氏より「BS7799 に準拠したセキュリティポリシーマネージメント」について、ご講演いただいた。
④ 11 月には JUAS セミナーが開催され（聴講は希望者のみ）、富士通（株）田淵氏より「IT セキュリティ国際標準 IS/IEC 17799 と BS7799 の管理項目の事例」を講演していただいた。
⑤ １月には日本アイ・ビー・エム（株）大木氏より「ネットワーク社会と情報セキュリティ」について、ご講演いただいた。

①から⑤により BS7799 を理解し、当初の目的、つまり論理的に情報セキュリティ管理を考えることができるようになった。残る課題は、リスクマネジメント意識の低い企業におけるセキュリティポリシーの策定であり、共通の課題は策定したポリシーを社員にいかに守ってもらうかである。

これから記述する内容は研究部会メンバーの議論をまとめたものである。実践的経験に基づいているので書物からは得られない貴重な参考書である。

第 2 章　リスクマネジメントの考え方

－いくつかの業種・業態の視点で－

現在、多くの企業は管理規定の上位規定である行動基準、機密管理規定等に準拠して、情報システム・ネットワーク・電子化情報をいかに守るかを、必要に応じて、場当たり的に規定を策定して運用している。リスクマネジメントの一環として人間系のリスクをも考慮した総合的なセキュリティポリシーを持っている企業はまだ少ない。また、業種、外資かどうかによりリスクマネジメントの意識が大きく異なる。

2.1　外資系企業の場合

セキュリティポリシーの策定に「トップを巻き込む」のが難しいという企業が本研究部会メンバーにも複数あるが、その感覚が私たちの会社からすると理解しにくい。外資系の場合、全社的なリスクマネジメントがいちばん上位にある。例えば「ポリシーを定めて守りなさい」というようなものが 40 数個ある。そのうちの 1 項目として、自分たちが提供している「社内の情報インフラ」についてセキュリティポリシーを定めて守りなさいとなっている。トップダウンで（社長命令で）行われているので、ボトムアップで役員を説得する必要があるということが理解できない。

2.2　金融機関の場合

金融機関については、その種類・会社数が多いため、一律同じ状況というわけではないが、金融庁が作成している金融機関（含む保険会社）への検査マニュアルにリスク管理に関する項目があるため、リスクマネジメントに対する関心は高い業界と言える。

特に、検査マニュアル上のチェック項目に「リスク管理の方針の確立」を確認するものがあり、①基本方針の策定状況、②基本方針の中にセキュリティポリシーを含んでいるか、③セキュリティポリシーには保護されるべき情報資産・保護を行う理由・責任の所在を定めているか、等がチェック項目としてあげられている。この項目に対応するために、レベルの差はあるが、各金融機関で種々の対応が行われている状況と考えられる。

2.3　情報サービス企業の場合

コンピュータのデータセンター会社は、セキュリティというものは技術的に対処すればよいという考え方である。

2.4 重厚長大産業の場合

日本の大手の重厚長大型産業では、リスクマネジメントの考え方を情報システムの運用管理に取り入れていないというのが現実である。危険が少ないのだから従来どおりでも構わない。せいぜい内部の社員や外注の操作員をしつけておけばよいという範囲のことだろう。

商売に結びつくところは早いが、情報系の部分は商売ではないので遅れる。しかし、実際にはワールドワイドにインターネットでつながっている。半導体関係の機械装置があるのだが、マーケットがワールドワイドであり、保守もワールドワイドで行わなくてはならない。完全に中まで入ってきてデータベースをクロスするまでは行っていないが、要求は出てきている。 パッケージソフトを導入して、システムをカットオーバーしようとしている段階である。工場でも高い機密保持を必要とするところは安全領域を設定し、部分的に指紋認証を使用して行っている。 しかし、ネットワークを利用したシステムについてはガードがなかなかできないという問題がある。

トップがビジョンとして述べても、具体的に噛み砕いてリードしていく人が出てこない。JUAS でこのようなプロジェクトを起こしてやったので、まさにいまポリシーができかかっているところである。そこまでもっていくのが難しい会社も多いと思う。

第 3 章　BS7799 を企業のセキュリティポリシーに適用する場合の考慮点－いくつかの企業では－

ある企業では、関連会社との電子情報伝達は（E メールに加え）Web アクセスで行う範囲にとどめている。LAN 経由では接続しないというのが原則であり、セキュリティポリシーで定められている。Web で参照されて困るものについてはアクセスコントロールをしておけばよいのであり、それほど難しくない。しかし状況が大きく変化してきている。関連企業の人たちが社内で開発作業をすることが増えたため、その人たちが接続する（例えば開発用の）LAN を独自に敷設し、それと当社 LAN との間をアクセス制御製品を導入・設置して接続している。

ただし、この場合はサーバーや運用管理システムが必要となり、かなりのオーバーヘッドになるので、大掛かりな作業に対してでなければ適用しにくい。このような仕組みでアクセス制御できている範囲はまだ狭い。アクセス制御がまだできていないところでの対応は、「あなたのアクセスしてよい範囲はこの範囲です。その範囲で業務をしてください」という書面を渡す。そしてセキュリティを守るという誓約書をもらっている。個人認証を行う CA センターを社内に立ち上げるということは、まだ検討段階である。

一方、別の企業では「セキュリティポリシーを作らなくてはならない」と大上段に構えるのではなく、自分のところでできる部分から始めることが大事だと考えている。極端に言えば、情報システム部の中のレベルを合わせるために、その中でできる範疇で作って実践して、その次にユーザーを巻き込んだり、ある事業部の中で行っていこうと考えている。情報システム部だけで考えて実施すると単に使いにくくなっただけであるという話も出てきたので、どういう段階でユーザーを巻き込んで情報収集を行わなくてはならないかということについても参考になった。

以上の例から次のような結論が導き出せる。

セキュリティ先進企業のセキュリティポリシーは、必要な規定を必要になった段階で策定し、導入している。その集合体がセキュリティポリシーである。BS7799 と比較すればポリシーの網羅性は低いが、その企業の言葉で書かれた、その企業の文化にあったポリシーである。つまり、BS7799 が ISO 化されたからといって、その条項すべてを規定化しても社員のセキュリティ意識が変わらなければ意味がない。企業文化に合ったポリシーを PDCA（Plan/Do/Check/Action）のサイクルで改善してくことが、経済的で効果的なリスクマネジメントにつながる。

第４章　何故セキュリティポリシーが必要か？　誰のためのポリシーか？　－法律家（弁護士）の視点で考えると－

4.1　情報セキュリティ対策は何故進まないか

トップも頭ではセキュリティの必要性がわかっている。しかし彼らの中に優先順位がある。OA に金をいくらかけたらいいかという標準がなく、不安だからと金を支出して、得られる効果が不透明なものに対して、どこまで責任を負うかというプレッシャーがある。 一方には世の中の動きがあって、もう一方には現実のビジネスがある。規模が違う。

セキュリティに関する事件では、せいぜい何百万か何千万円の事件がときどき起きるだけである。あとは普通の事件である。セキュリティ問題があったために著作権が発生して不正競争になってしまったというような事件である。それはそれで訴訟を行う。大きくなるかもしれないが、ケースとしては少ない。

そして一方では、これだけ投資したらこれだけの儲けになるという現実があって、そのためにこれだけの金が必要だといわれたら、優先順位としてはこちらに金をかけたくなる。

これを変える必要があるとは私は思わない。しかし、本当に変える必要があるとしたら、ボトムアップで説得する技術が必要になる。

どうしてセキュリティ対策が進まないのか。すでに出来上がっているところからすると不思議な話だろうし、また、現在作ろうとしているところからすると、どうしてそんなにうまくいったのかと思う。そのようなギャップがある。実際に私自身もいろいろな会社を見ていてギャップを感じる。業種を問わず、また IT に近いか遠いかを問わず、ルーズなところと鋭敏に反応するところとある。それは、トップあるいは従業員の感覚の違いである。すなわち、企業人というのは、一般的に「右手に利益、左手に理念や希望（自分の活動を通じて社会に貢献するというような理念や希望）」を持っているが、その矛盾の中で日々が過ぎていく。そのバランスがどの辺に振れるのかという問題である。

4.2　企業活動における重要性判断の基準は何か

セキュリティポリシーやスタンダードを作ってそれを実現すればいいという議論は、訴訟や争い事を前提としたり、他人に自分のことを説明する、すなわち防御するという側面が強くなる。トップの威光が非常に濃厚な個性的な企業、すなわち老舗のようなところでは、「おれに任せろ」というような面があるので、セキュリティポリシーができるかどうかがはっきりする。しかし、そういう企業はトップが責任をとってしまうので、セキュリティポリシーは本当はいらないのかもしれない。

大手の会社、例えば金融機関は外部的な監査・監督の基準があるので、当然のことのよ

うに行っている。メーカーやその他の領域の一般的な会社では、確かに 2 つに分かれている。外国との接点があったり歴史の古い会社では、何かあっときには自分で腹を切って責任をとるという備えがあるように感じる。例えば、財閥系の企業と話していると、企業といっても企業グループという感覚であり、どんな危機が来ても、どこかで吸収できるという自負があるように思う。正面切って危機を捉えるというような危機感というより、むしろ美学を追求するところがあって、美しいからやってみようというようなことであり、切迫性がない。ある財閥系の企業では、グループの中の金融機関は行うが、メーカーは行わない。

「自分はこうだから責任を負わなくてよい」という行動原理を是とする会社かどうかによって異なる。日本の会社の経営者のスタンスは「責任は取れる範囲で取ります。どこまでも取ります」というものであり、そして「できないものはできない」ということになる。外資の会社のように「これをやっているからいいじゃないか」というものの考え方はしない。スタンダードを作っておいて、「これだけやったんだからいいじゃないか」といった自己弁明を前提に塀を作り、それをやっているかやっていないかで議論するという風土は薄いという気がする。だから、なかなかすんなりとは入っていかないのだと思う。

もうひとつには、日々、大事なビジネスがあり、稼ぎの単位が大きい。稼ぎの単位とセキュリティ問題にかけるべき量あるいはそこで想定される被害とを比べると、やはり日々のビジネスのほうが頭の中に多くを占めることになる。

事件が起きたら警察に頼もうとか弁護士を呼べばよいというような、伝統的に行われてきた危機への対処の仕方が、ここにも現れてきている。すなわち、積極的に防衛しようという感覚はない。

4.3　セキュリティ対策と責任論－リスクの把握と評価を巡って

(1) どのようなリスクがあるか、そのリスクが誰に、どう影響するかの道筋を明確化する必要がある

1)会社

①損害賠償請求、差止請求、取引途絶、マーケットの縮小、株価の下落、マスコミリスク、金融信用の失墜など、想定されるリスクの数量化

②数量化された結果と決算の関係を評価させる

私は法務部の顧問だが、法務部を経由してくると、法務部に現場が相談に来る。両者とも真剣に考えている。法務部はマスコミリスクや市場リスクに関心が高い。どういうリスクがあるかは、現場でなければわからない。大事なことは、リスクが何かということを把握すると同時に、それが誰にどういう責任を及ぼしていくのかという筋道である。誰が何の責任を負うのかという筋道を特に現場の人にはっきり理解させる。すなわち、トップが何もしないために、あるいはトップがすべきことをしなかったために会社に損害を与えた

場合は、1 株でも株主が裁判所に 8,200 円の印紙を貼って出せば、その社長はこの間の例でいえば 15 億円あるいは 500 何億円の損害賠償に応じなくてはならなくなる。このようなことを説得のために詳しく知る必要はないが、いずれにしても、株主の 1 人が会社の損害を取締役個人に対して非常に簡単に請求できるようになっていることは理解しておいてよいだろう。

2) 取 締役・監査役責任の明確化

①商法 266 条　会社に対する取締役の責任

②商法 266 条の 3　第三者に対する取締役の責任

③商法 267 条　株主代表訴訟（印紙代 8200 円で可能）

トップは技術の問題になかなか入り込めない面がある。結局、経営者は何を考えているかというと、利益なり決算なり、将来的な収支の問題にこの問題がどう響くのかということである。いったい誰にとってのセキュリティポリシーなんだというところが非常に生々しい。変な情報が Web に流れて「あなたのところの信用が落ちて株価が下がって首が飛ぶよ」という危機感があれば一所懸命になる。「あなたのところにセキュリティ対策がないから、うちの情報が流れた」ということで首が飛ぶ、つまり人生が否定されるというところまでいけば、役員は一所懸命に行う。

株主総会にしても、代表訴訟というものができて、現実的に代表訴訟が起こされるようになってから、総務部がお膳立てした総会対策の打ち合わせの日と、社長のそれとでは雰囲気が違う。今までは、総務部がお膳立てした場に社長が来て打ち合わせをして帰っていったが、最近は総務がお膳立てするのを社長が見ていて、総務が帰ってから、社長が本来の時間ではないのにわざわざ来て「あそこではこうだったが、本当はどうなのか」「これで本当に自分は代表訴訟を耐えられるのか、また個人の損害賠償を耐えられるのか。本当に大丈夫か」と聞いてくる。すなわち、私たちが会社の味方なのか、取締役の味方なのかを大変気にしている。法律的にいうと、代表訴訟で役員が責任を負わなくてもよい領域と会社が免責される領域とは、実は矛盾する場合がある。したがって、正確に答えようとすると「あなたは経営判断をした人として責任を負わなくてはなりません」と言うしかない。「そのリスクは社長を辞めるか続けるかで、あなた自身が選ぶしかない」ということになる。すでにそのことに経営陣は気がついている。あるいは何らかの危機が生じたときにそういう問題が起きるということは、いろいろな想定の中で、あるいは株主総会や業界の動きの中で知っているはずである。要は、その中に情報セキュリティの問題やセキュリティ一般の問題が入るかどうかということであろう。

3) 従 業員

就業規則に基づく懲戒・解雇・不利益取扱の明確化。

(2) リスク評価作業

1) リ スク評価基準の決定者

リスク評価の基準、リスクの可能性の多様性に照らして、企業トップ以外にない。リスク評価は企業のポリシーの宣言であることを意識すべき。

企業トップがセキュリティ対策を必要と考えるかどうかの観点は、本当のことを言えば“わが身”である。その次が会社、そして業界であろう。これは利益や哲学など全部を含めた意味である。リスクを把握するという最も困難な点について何を基準に把握するかというと、わが身にとってどれだけ危険なのか、あるいはうちの会社の 2 年間、あるいは 1 年間の決算にとってどれだけ役に立つのか、あるいは危険なのかということである。そのような具体的な項目を立てて検討していくことが比較的有益である。

2) リ スクの評価作業を行うのは誰か

直轄の評価部隊と担当部署の交渉。この交渉を通じてリスク評価が徹底する。

実際にリスク評価の作業の中心を担うのはシステムの人間と危機管理の部署の人間であるが、そういう環境のもとにあるということを十分に知らしめることによって、「リスク評価をするのはあなたしかいませんよ」と伝える。 最高の危機管理責任者は企業トップである。リスク管理に関する書物でも、あるいはアドバイザーに意見を求めても、リスク管理の責任者はトップである。そのことはわかっているだろうが、問題はリスクの把握と評価である。「把握はこちらがするが、評価はあなたです」と、孤独なところに追い詰めなくてはいけない。「右か左か」と迫っていく中で、それぞれがリスクを把握したり、評価するにあたって、当然、議論していく中で、セキュリティポリシーの監査の問題も含めて、全社的に実施する環境が整っていくのではないかと考える。

では、リスク評価をするのにどういう基準があるのかということで、BS や ISO を持ち出すのだが、はっきり言って、それらを生の形で経営者に示したところで、「こんなものはわからない」ということになる。ばらっと見てみると当たり前のことが書いてあって、いったいどうすればよいのかということになる。経営陣に話をするときは、「このプロジェクトにはこういう危機がある。誰かに入られて、今の段階でこれを盗まれたら、この計画はだめになって、これまでプロジェクトにかけた情報は全部なくなる。これによる稼ぎの見込みは全くなくなる。場合によっては、こちらがあとで作れば不正競争とみなされることがある」という現場のシビアさを一つ一つ提示していくのが一つの方法である。そして、具体的な技術はこちらに任せろと言ってシステムのほうに引き取るべきである。具体化するスキルがない人にポリシーについて述べてもわかってもらえないので、安心をさせるためには「それについては国際標準があって、それに従って行うしかない」と言うしかない。

4.4 免責の基準をどう把握するか

(1) 基準の有無の把握

アメリカの連邦最高裁判所も州の裁判所も、今の段階では、セキュリティポリシーを作っていればすべての場面で免責されると言っているところはない。具体的なそれぞれの事件でそれぞれの場面を考える。国際標準自体もやっと作られたものであり、不確定である。

したがって、他の事件との関係で考えてみると、弁護士として言えることは、医療過誤や建築紛争とよく似ているということである。

建築紛争から学ぶべきことは、欠陥や瑕疵があるということをどう表現・認定していったかという点である。金融公庫の標準仕様や建設省の大臣官房の出している標準仕様書、日本建築学会の仕様書、建築家団体の仕様書、あるいは JIS というスタンダードによる。これらは内容的にはほとんど同じであり、それらが基準になる JIS では、ネジの切り方から、付け方から、溶接の仕方など全部について基準がある。建設の場合であれば、「柱のこの部分の溶接については JIS で、溶接基準はこうだ」というように議論していく。試験方法ももちろん豊富に揃っている。そういう意味では JIS や ISO を基準として議論され出している。

医療過誤訴訟の場合は、相手が死んだり生きていたり生身の人間であって多様性があるので、JIS のようなものでは把握できない。それぞれの医療水準論というものがある。大学病院は最高能力を有していると社会的に考えられているので最高の水準であり、この場合は海外の文献も含む。町医者の場合は、そこまではいかない。

(2) 基準がないもの

免責の基準をどう立てるかは極めて複雑であり、考えられる法益侵害の防止のレベルまで落とす必要がある。

1)内部情報の漏洩による営業機密の漏洩→不正競争防止法による差止・損害賠償

もうひとつは、情報漏洩で営業機密が流れて、製品化されてしまい不正競争になってしまったという例は多いので、それによる損害賠償の可能性を提示する。そして免責の基準を示す。これについては、所轄の部の法律家に聞けばわかる。

2)従業員のミスによる著作権の侵害→著作権法違反による差止・賠償賠償

第 5 章　ポリシー策定を成功させるためのプロジェクト活動事例

5.1　ポリシー策定のためのプロジェクト活動

各事業所のシステム部門のメンバー13 名を集めて、プロジェクトを実施し、現在、基本方針と対策基準からなるセキュリティポリシーをまとめている。メンバーは専任ではなく、1・2 回／月会合を行い、4 か月程度の活動を予定している。また、先行している事業所もあったので、そこで作成したものをベースにして全社版を作成するといった形式で活動を実施している。

このプロジェクトを始めるにあたり活動趣旨を説明した際、「顧客からセキュリティポリシーを求められる可能性があるから、ぜひ実施して欲しい」という意見が事業所からも出され、活動はすんなりと始められた。しかし、ポリシー策定を成功させるためには、この活動をシステム部門だけの活動ではなく、社としての活動としてどれだけ進めていけるかが課題だと考える。

実際に総務部門・法務部門と接触を開始しているが、以下の点を説得材料とした。第 1 に、インターネットを利用したネットワーク接続が急増しており、不正アクセス等の問題が身近になってきており、対策が必要であること、また、セキュリティポリシーを持っていない会社とはネットワーク接続をさせないという企業も出てきており、今後のビジネス展開で支障が出てくることも考えられること。第 2 に、セキュリティ管理の国際標準化および JIS 化が進んでいること。第 3 に、政府が「セキュリティポリシー作成のためのガイドライン」を作成し各省庁に対しセキュリティポリシーを作成するよう指示を出したり、また「重要インフラのサイバーテロ対策に係る特別行動指針」の中で重要 12 分野を特定し、この分野の民間企業に対しても先のガイドラインに沿ってセキュリティポリシーを作成するように指導していること。

以上のようなことを説得材料とし、セキュリティポリシーを策定しなければならないということを納得してもらい、現在一緒に内容の確認等の活動を進めている。

またセキュリティポリシーでは、基本方針や対策基準を記述するに留め、具体的な対策や方法は、別に運営要領や技術標準等を定め、そこに記載する予定にしている。そうした運営要領・技術標準を整備するといったポリシー定着化の活動も今後必要になるであろう。

たとえば、ソフトウエアのライセンス管理に関しては、セキュリティポリシーでは「事業所毎にソフトウエアのライセンス管理責任者を設け、著作権法等に違反しないよう、ライセンス数と導入パソコンの対応を管理する」という表現にしているが、実際にどうやってライセンス数と導入パソコンの対応を管理するのか記述したものがまだないという現状である。また、電子認証にしても「重要な情報をやりとりするシステムでは電子認証等を用いてセキュリティ確保をする」という記述にしているが、電子認証の仕組みをどう構築するべきかという指針を出さないと、実際には管理が回っていかない。そのためセキュリ

ティポリシー作成後 1 年間程度は、具体的な施策を提示するようなポリシー定着化のための活動をしていく必要があると考えている。

5.2 セキュリティポリシー策定のノウハウ

朝日新聞のセキュリティポリシー作成の苦労についてのフォーラムを要約すると、「守られないものを作ってもしようがない。難しいものを作ってもしようがない。守ってもらうためには、解説書のようなものを付けるとか、作れるようなものしか作らないことである」。

BS7799 の項目を全部行うという方向の考え方とは大分違うようである。

情報システム部とは部門が違うところへ適用するポリシーの策定はどうするのかという質問があったが、次のように対応した。

例えば営業部門には営業部門を束ねる部がある。その部に、営業部門でどういうことを守らなくてはならないかという観点から営業部門向けのポリシーを策定してもらう。同様にフィールドで働いている SE 部隊を束ねる部には、フィールドで働く SE 向けのポリシーを策定してもらう。ソフトウエア部門にも同様に部門向けポリシーを策定してもらう。セキュリティポリシーは、このようなものの集大成である。情報システム部が策定したものもあるが、それだけではない。

社内ですべてのことを行うことを前提としたポリシーを作るのか、アウトソーシングを前提としてポリシーを作るのかによって、ポリシーの作り方は異なる。情報システム部の人間は、しょせんパソコンマニアであって会社の役に立たないから雇いたくないという強烈なことを言う社長がいたが、そういう会社では、基本的にはすべてアウトソーシングで、社内はそれをコントロールする人間がいればよいという考え方である。そういう会社は最初からそういう形でポリシーを作る。

問題なのは、ある事業部やある分野では極力社内で行い、それ以外ではできる限り外注したいというようにばらつきがある場合である。どういうときにアウトソーシングをして、どういうときにアウトソーシングしないのかという基準、さらにアウトソーシング先をコントロールする基準がばらついてしまう。

第６章　ポリシーを守らせるためのノウハウ

セキュリティポリシーを導入しても、なかなか守られない。罰則規定の適用が甘い日本企業の文化に起因するものである。次の例は、その点を工夫した企業からの紹介である。

情報セキュリティの監査に関しては、部門の自己監査というのが定められている。情報セキュリティ委員会で監査項目を定める。監査室も情報セキュリティ委員会のメンバーであり、専門家である彼らを中心に自己監査基準・手順を作成する。この基準・手順を情報セキュリティ委員会で承認し部門へ配布する。前回の監査では、これらの自己監査の基準・手順に関する事前の講習会の必要なしと判断され、支援窓口を設けることで対応した。数十件のＱ＆Ａがあった。これから判断すると自己監査の基準・手順の事前講習は必要である。

部門から監査報告をもらったあと、部分的な抜き取りの実査を行い、次回以降の自己監査に反映する。

何回か、このような形式で自己監査を継続して実施していき、将来は部門ごとに監査項目を選定し、年間スケジュールを立てて実施できるところまでもっていきたい。

それは非常にいい方法だと思う。例えば、今は株主総会の想定問答集を作成する時期だが、「お宅の会社では、セキュリティ対策はどうなっているのか」と聞かれたときに、「行うべき基本的な項目を決めて、各部門に実行させている」と答えることができる。役員、取締役の責任は何かというと、適正に行われているかどうかを管理することである。細かいことはどうせわからない。同じ責任だと言える体制になっている。これが現実だと思う。役員は危機管理の第 3 ラウンドは、絶対にわからない。彼らの責任がどこで免除されるかというと、結局は一般的に承認された方法で危機管理を行っているかどうかである。それ以上のこと、すなわち出かけていって蓋を開けてネジを回してというところまで求められるはずはない。そういう意味では有効な手段である。

第７章　世の中の動き

ISO17799についての経緯とISMS（情報セキュリティ管理システム）について

1995年　　BS7799が英国標準規格として発行
1998年　パート1（ガイドライン）、パート２（情報セキュリティ管理システムのための仕様）の２部構成となる。
1999年　　改定
2000年12月　BS7799のパート1がISO17799として発行
2001年 4月　日本においてISO17799を参照した（実質的にはBS7799パート２）、ISMS適合性評価制度の運用を開始。
これに伴い、情報システム安全対策実施事業所認定制度（安対制度）をISMSに統合廃止。
ISMSの維持管理は、JIPDEC（日本情報処理開発協会）が行う。

第８章　まとめ

　ネットワークの普及、EC の普及、国際標準、認証制度の制定、人の流動化、株主訴訟、政府の指導等を考慮し、特に企業トップの意識向上を図り、企業にとって意味のあるセキュリティ対策およびポリシーを策定していく必要がある。

●参考資料

(1)IT セキュリティに関する国際標準

・BS7799-1:1999,BS7799-2:1999　英和翻訳版　日本規格協会

・「国際セキュリティ標準 ISO/IEC17799」田淵治樹著　オーム社

・JIS X 5070 (ISO 15408 の JIS 化)

(2)金融機関に関するもの

・FISC 基準　財団法人金融情報システムセンター

・「金融情報システム白書」財経詳報社

(3)ネット上で標準を掲載するもの

・総務庁 HP　　行政情報システム安全対策

・官邸 HP　　情報セキュリティに関するガイドライン

・電脳火消隊　　http://www.firewall.gr.jp/rilatedlinks/policy-links.html

・IPA HP　　情報セキュリティの現状　2000 年版

　　情報システム部門責任者のための情報セキュリティブックレット

補足寄稿文

法的視点から見たセキュリティ対策
なぜセキュリティポリシーが必要か、誰のためのポリシーか？

弁護士 **稲垣 隆一**

本寄稿文は本報告書 第４章について理解のしづらい箇所、正確性を欠いていた箇所、補足説明を要する箇所を見直していただいたものである。ご苦労いただいた、弁護士 稲垣隆一氏に感謝申し上げる。

（セキュリティポリシー研究グループリーダー　岸本 佳宏）

１．情報セキュリティ対策はなぜ進まないのか？

トップも頭ではセキュリティの必要性はわかっている。トップがセキュリティ対策に積極的でないとしたら、それは、セキュリティ対策が投資の優先順位の中で他のものに劣後するからである。セキュリティ対策が企業活動に及ぼす影響、収益を増大させる効果、株主、資本市場、取引市場に対する重要性、トップの責任に対する重要性などの要素は、投資の優先順位に影響を与える。セキュリティ対策についても、これらがはっきりすれば、対応は進む。例えば、Y2K 問題への金融機関の対処を振り返ると、あの時は、金融監督庁からの指示、全銀協の取り組みといういわば外圧があり、実際のトラブルが発生した場合の混乱、責任問題など、トップから末端の社員にいたるまで、対処を怠ればどのような不利益が誰にどう生じるかがある程度はっきり認識できる状況があった。そのために、未だセキュリティ対策の具体的手順までは持たない企業においても、Y2K 問題を回避するための限度では、極めて具体的な手順まで定めた対処が行われた。

どうしてセキュリティ対策が進まないのか。「すでにできあがっているところからすると不思議な話だし、現在作ろうとしているところからすると、どうしてそんなにうまくいったのかと思う」という話がある。しかし、第３章の末尾の考察にも、セキュリティ対策が進んでいる企業では、最初に把握すべき「リスク」を、役員から末端の社員に至るまで、経営や責任の視点からも詰めることに成功していることがはっきり現れている。弁護士の視点でセキュリティ対策がなぜ進まないのかを分析しても同様で、セキュリティ対策を怠った場合の経営や責任の問題が存在しないか、存在しても、トップや社員がはっきり把握できないでいる企業においては、そこがボトルネックになってセキュリティ対策は進まないといってよい。

その意味で、「セキュリティ対策を怠っても、本当に経営や責任の問題が生じないなら、セキュリティ対策は不要である」という意見は傾聴に値する。

セキュリティ対策担当者は、ボトルネックになっているのがトップであるのか、従業員であるのか、組織的にどういう部署なのかを見据え、これに応じて組織全体の関連の中でセキュリティ対策の要否を判断し、もし必要であるなら、これを怠った場合の経営や責任論からの説得の技術を磨くことが有益である。そこで、以下、こうした視点から、セキュリティ対策を怠った場合の責任がどう生じるか、これを具体的にどう把握するかなどについてさらに検討してみる。

２． セキュリティ対策と責任論

２.１１　経営や責任論からリスクを把握するとは

経営や責任論からリスクを把握するとは具体的にはどうすることか。その中核は、これまで技術的なリスクとして把握されたことがらを、技術的リスクをカバーしないことによって、誰がどのような責任を負うことになるのかを明らかにすること、つまり人のリスクとして捉え直すことである。いくら技術的脅威があっても、それが企業活動や人の責任を発生させ、不利益にならなければ、そこに投資する必要はない。そのようなものに投資家から付託された資源を投資することはむしろ許されないというべきであろう。

そのためには、以下の４点を意識して、ターゲットとする部門、関係部門との協議を行うことが重要である。

第１点は、情報セキュリティの不存在や不備による技術的なリスクがもたらす企業活動上の「不具合」を把握することである。これを現象別に大きく捉えると、①セキュリティ対策が存在しないか不十分なことそれ自体が不具合となる場合、②システムそれ自体や情報が破壊され、あるいは情報が改変・漏洩したことにより会社に生じる不具合、③それらの不具合により会社が取引先第三者に損害を与えた場合及び④第三者がこれらの事情を生じさせた場合に会社（役員・従業員も含む）が荷担したと評価される場合あるいは会社が第三者と同視される場合などが考えられる。このうち、①セキュリティ対策それ自体が存在しない場合による不具合の場合の例としては、EU指令に拘束される国の企業との取引においてこちら側に個人情報保護体制の１つとしてのセキュリティ対策が講じられていない場合や、新たな取引の引き合いがあったり、これまでの取引先が新たにセキュリティ対策を講じた場合に、会社のデータセンターのセキュリティ対策水準の不備を理由に、取引を途絶される場合が考えられる。また④の会社の荷担の事例としては、会社が踏み台となった場合、外部委託先が情報の破壊・改変・漏洩を行った場合でも、会社が外部委託先のセキュリティ対策が不備であることを看過してこれに委託した場合などが考えられる。

第２点は、こうした不具合がもたらす損害はどこにどのように生じるのかを明確にすることである。不具合は、例えば、損害賠償請求、差止請求にとどまらず、取引機会の喪失、これまでに築いた信用の喪失、取引途絶、取引市場における評価下落、資本調達市場における株価の下落、マスコミリスク、金融機関からの信用の失墜など多岐にわたる。これらの不具合がどのような損害をもたらすのか、また、その損害はどこにどのように生じるかを具体的に把握する必要がある。そのためには、関係部署と十分な協議をする必要がある。

第３点は、これらの不具合のもたらす損害が企業会計上どう影響するかを把握することである。企業会計上の影響を把握するには、社内の財務会計部門はもちろんであるが、場合によっては監査法人の意見を徴することを要する場合もあるであろう。

第４点は、これらの不備が、誰のどのような責任に結びつくかを示すことである。 その前提として、関係者がどのような根拠により責任を負うかを以下に示す。

【取締役】

ア．商法２６６条　会社に対する取締役の責任

イ．商法２６６条の３　第三者に対する取締役の責任

ウ．商法２６７条　株主代表訴訟（印紙代８２００円で可能）
エ．民法７０９条　一般不法行為
オ．民法７１５条２項　従業員の不法行為に対する代理監督者責任
カ．民法７１９条　共同不法行為責任
（ 子会社取締役と親会社取締役の共同不法行為が問題となりうる）

【従業員など】
ア．労働契約にもとづく損害賠償責任
イ．就業規則にもとづく懲戒・解雇・不利益取扱の明確化
ウ．身許保証人の責任は、本人の責任のうち、限定された限度にとどまる。

２．２　例題

以上の処理を、セキュリティ対策部門が、開発部門の情報漏洩対策を行おうとする場合を想定して考えてみよう。

セキュリティ対策部門は、開発部門における情報漏洩リスク対策が行われていないことを把握した後、技術的なセキュリティ対策の叩き台を作成するとともに、開発部門と、これを欠いた場合の不具合の内容、例えば、開発競争に敗れるという不具合、その他どのような不具合があるかを洗い出す。さらに、開発部門の収支管理部門と、この不具合により生じる損害として何があるかを洗い出す。その際は、開発費など具体的に計算される費用の喪失、開発計画の段階で計画された収益の喪失、業界や社会からの評価下落、従業員の志気の低下など、具体的に把握できないものも含め、どのような損害が生じるかを検討する。

さらに、セキュリティ対策部門は、これらの検討に、例えば、事業本部、営業、総務などの関連部門を加え、全社的に、現時点において開発部門においてセキュリティ対策の提案する対策を講じなかった場合の不具合と損害額を評価する。

その際、取引途絶や業界内における評価下落などによる損害を把握するには、営業部門からの意見聴取が有益であり、株主対策や IR・広報上の利益・不利益は、その担当部門からの聴取が不可欠である。損害は、企業会計上の処理を通じて企業における意味が確定される。したがって、損害額の把握にあたっては、財務会計担当部門との協議も有益である。損害額は短期・長期、計算可能・計算不能のものに分けることも有益であるが、企業ごとに計測の基準を詰めていく必要がある。また、セキュリティ対策を実施する人の管理・対策を怠った場合の制裁の程度についても、担当部署・人事労務担当部署とも協議を行う。これは、担当部門内の職員にセキュリティ対策の必要性、重要性を理解させ、後の制裁規定や就業規則改正作業の準備に資することになる。さらに、誰がどのような責任を負うかについても、明らかにしていく。上の例では、担当役員及び取締役会構成員たる取締役は、監督責任はもちろん、情報漏洩を想定してその対策を講じなかったことによる会社の具体的損害、監督官庁からの規制による不利益、マスコミ報道されることによる損害、業界における損害、広告宣伝費の無益化などにより、株主総会で株主からの責任追及を受けるばかりか、場合によっては、会社から商法２６６条に基づく損害賠償責任、代表訴訟による個人責任の追求を受ける可能性があることを明らかにする。また、情報を漏洩させた職員、情報管理担当の職員、部門長は、会社に対して責任を免れず、労働契約上の懲戒の制裁、損害賠

償責任、人事考課上の不利益処遇の責めを負うことも明らかにする。

受託した事業において情報を喪失・改変され、あるいは漏洩されたことによって委託先企業に損害を与えたときは、当然、会社は取引先から損害賠償を受け、担当者、部門長、担当役員、取締役は、責任を追及されることになることも明らかにする。

このようにして、対象となる不具合とこれによる全社的損害の把握が行われると、例えば、情報漏洩対策のためにどれほど口うるさい規定を作るべきか、制裁としてはどの程度がふさわしいかという悩ましい問題も自ずと解決されてくる可能性がある。全社的把握がなされると、例えば、よく厳しすぎると言われる「管理区域外においては、その業務の取扱から得た事実を、許可権者の書面による事前の許可なく、社内外人を問わず第三者に漏洩してはならない。」などという規定を定めることや、これを遵守させることも容易になり、この違反に対するペナルティをどうするかについてのコンセンサス（比例の原則＝不利益は会社に対して与えた被害に比例するものでなければならない）も得やすくなるであろう。

２．３　セキュリティ対策部門の位置づけ　代表取締役をトップとする全社的危機管理部門

こうした協議を経てトップが資源決定配分をする際の資料を積み重ねていく。セキュリティ対策部門が対策を樹立するにあたり、リスクが発生する可能性のある部門だけでなく関連する部門と検討を行うことを通じて、これらの部門にセキュリティ対策の重要性を理解させ、ボトルネックとなっていた部門がセキュリティ対策やその実施の価値を具体的に把握できるようにすることは、対策樹立後の実施効果や監査成績をあげるためにだけでなく、実際にセキュリティ対策を実効あるものに練り上げ続けることに役立つだろう。また、このような各部門を巻き込んだ協議体制が作られていく過程で、各部門の責任者がトップを巻き込んで協議をせざるを得なくなる。その結果、このような検討過程は、とりもなおさず、代表取締役を頂点とする直轄のセキュリティ対策部隊の構築過程に他ならなくなるであろう。

２．４　リスク評価作業　リスク評価の最終決定者は誰

このようにしてリスクが把握された後は、セキュリティ対策の実行を決定する段階に至る。リスク評価の基準を見いだすのは、上記のように、リスクの可能性の多様性に照らして、代表取締役以外にない。リスク評価は企業のポリシーの宣言でもあることを意識すべきである。

セキュリティ対策担当部門が、トップにセキュリティ対策実施を決断させられない悩みの多くの原因が、トップにとって、リスク評価を行う場合の基準が不明確であることであったが、関連部門との協議を通じて、技術的リスク、経営、責任論からのリスク把握を示した後に、経営資源のうちどの程度をセキュリティ対策に割くか否かの決定は、専ら経営判断事項であり、その決断は、代表取締役、程度によっては取締役会がこれを行わざるを得ない。

３．　免責の基準をどう把握するか

３．１　基準の有無の把握

取締役の責任の発生する根拠となる民商法の法令は上記のとおりである。取締役は、「法令」「定款」に違反して会社や第三者に損害を与えたときは、これに対して損害賠償責任を負う（商

法２６６条、同２６６条の３、民法７０９条)。取締役に対し、会社に特定のセキュリティ対策実施を義務づける法令は現時点では存在しない（もっとも、今国会において審議予定の個人情報保護法が制定されると、会社に対して一定程度のセキュリティ対策が法令上必要とされることが規定される可能性がある)。

しかし、会社との間で委任契約にある取締役は、その委任事務の遂行にあたり善管注意義務を負い、忠実義務を負う（商法２５４条３項、民法６４４条、商法２５４条の３)。これらの義務は、商法２６６条１項５号の「法令」に含まれるものと解されており、取締役がその職務執行にあたり、善管義務、忠実義務違反に違反して会社に対して損害を与えたときは、会社に生じた損害を賠償すべき義務を負う。第三者に損害を与えたときも同様である（商法２６６条の３)。さらに、民法７１５条２項の代理監督者の責任においては、十分な監督を尽くしたことを取締役側が立証しない限り、被監督者の不法行為についての責任を負うことになり、商法の立証責任は取締役側に不利益に転換されている。

セキュリティ対策の実施に関する取締役の判断は、会社の経営資源をセキュリティ対策のためにどこまで割くのが会社の利益にあたるかという経営上の判断であり、その判断が誤りかどうかは、取締役の善管注意義務ないし注意義務違反の問題とされる。（なお、アメリカ法において、そもそもリスクを伴う会社経営については、一定の条件のもと、裁判所は取締役の経営判断の当否に介入しないという「経営判断の原則」（Business Judgment Rule）は、日本では採用されておらず、単に、善管注意義務の判定にあたって、取締役の経営上の判断に一定の裁量権を尊重するというにとどまる。）

セキュリティ対策の実施の不備、実施しないことについての監督の不備、セキュリティ対策不備の見落としが、どのような場合に、善管注意義務に違反するかについて正面から判断を示した裁判例は今のところ見あたらない。しかし、他の事例においては、善管義務ないし注意義務違反の判決例が蓄積されており、これらの検討によれば、経営上の合理性を欠くことが明らかであるときは、責任を免れない。そのため、取締役は、その経営上の判断にあたり、自らの合理性を基礎づける根拠を収集しておく必要がある。

３．２　基準があるもの

セキュリティ対策が、ISO、BS、JIS などの基準に適合する内容で提案され、しかも、それが、各部門との協議の結果練り上げられた結果が示されて、これを欠くときは相当の損害が発生することが想定された場合は、これを拒絶する合理的根拠を持ち得ない限り、想定に従った損害を生じた場合に取締役の責任を免れることは困難となろう。他方、セキュリティ対策の内容が、ISO、BS、JIS などの基準に適合する内容で提案されこれを実施したにもかかわらず、損害を生じたときは、その判断が経営上の合理性を欠くことの立証は困難となり、取締役の責任を免れるための有力な武器となろう。もっとも、これらの基準に基づいて、会社独自の基準でセキュリティ対策を行ったときは、想定される不具合、損害との関係で、会社の基準設定の合理性を検討した結果を跡づける資料を準備しておくことが必要であろう。

これらの国際標準の現時点における法的意味のうち最大のものは、ある会社における通常のシステムを明らかにして責任発生の有無を明確化できることと、将来の訴訟に備えて証拠を収集で

きることである。また、類似の裁判と比較しても、こうした国際標準にのっとった自社基準の策定・実施、監査実施などの事実は、責任の所在を明らかにし、免責の基準としてきわめて有効に働くであろう。

３．３　基準がないもの

ISOなどの基準のないものについては、判例や判決例などを基準に具体的な防御策を講じる必要があり、結局は、上記独自基準による場合と同じになる。

３．４　危機管理部門の必要性

基準の有無に関わらず、問題は、経営上の判断に関する取締役の責任の問題を提起する。しかも、この分野に関する裁判所の明確なガイドラインはないといってよい。したがって、セキュリティ対策の樹立やその内容、程度を見極めることは、将来のリーガルリスクにどう備えるかという危機管理をどの程度行い、どの程度の証拠で、将来の訴訟を戦い抜くかという問題であり、総会対策や IR 対策をどう行うかという問題を抜きに考えられない。したがって、トップにより統括され、全部門、特に、法務部門、総務部門、セキュリティ対策樹立や管理、監査に通ずる顧問弁護士により組織された危機管理部門の充実が望まれる。

セキュリティ技術研究グループ

ネットワークセキュリティ技術の実践的研究

第１章　はじめに

当研究グループは、ネットワークセキュリティの技術的側面に絞って調査･研究を行った。ネットワークのセキュリティ技術と一言で言っても、その範囲は、コンピュータ室の保安対策のような物理的なものから、ネットワークデータの暗号化技術のような電子的なものまで、非常に多岐にわたり、かつ、それぞれの分野は深くて複雑である。

この分野には、すでに多くの専門書が出版され、市場にも多数の製品が出回っているが、ユーザーのシステム担当者から見れば、あまりにも情報が多すぎ、何を指針に選定し、どの程度まで実施すれば安心なのか、迷うばかりである。

このため当研究では､ユーザーのシステム担当者に必要最小限な情報を提供するとともに、少しでも実践的なセキュリティシステムの構築に役立つことを狙いにして活動を行った。専門的には物足らないところが多々あると思うが、ユーザーのシステム部門の技術者が気楽に読めて、セキュリティ技術の全体を俯瞰し今後の現実的な開発に参考になれば幸いである。

第２章　概要

話をわかりやすくするため、当研究では、インターネットを使った B2B ないし B2C のウエブシステムを運用する一般的なモデル企業を想定し（図２－１参照)、そこで用いられるセキュリティ技術を要素ごとにまとめた。一般にはこうした要素単位に製品があるわけではなく、多くは要素にまたがって機能を持つセキュリティ製品がほとんどであるが、考え方としては、要素単位の機能を整理することが基本であろう。

各章がその要素にあたる。また、技術を深く掘り下げるのではなく、平均的な一般的な技術レベルでのセキュリティを追求し、企業としてバランスのとれたセキュリティ装備が何かということを重視して、それを紹介することとした。どんな技術でも同じことが言えるが、セキュリティ技術も、セキュリティ能力と、それにかかる費用および利便性とは必ずトレードオフの関係があるからである。

第 3 章は、通信の対象が誰であるかを特定する個人認証の技術を取り上げる。ネットワークを用いた電子商取引システムでは欠かせない技術であり、21 世紀ネットワーク社会の実現には絶対に不可欠なものである。数多くの技術や製品が開発研究されているところであるが、ここでは、現時点での実際的な製品、技術を紹介する。

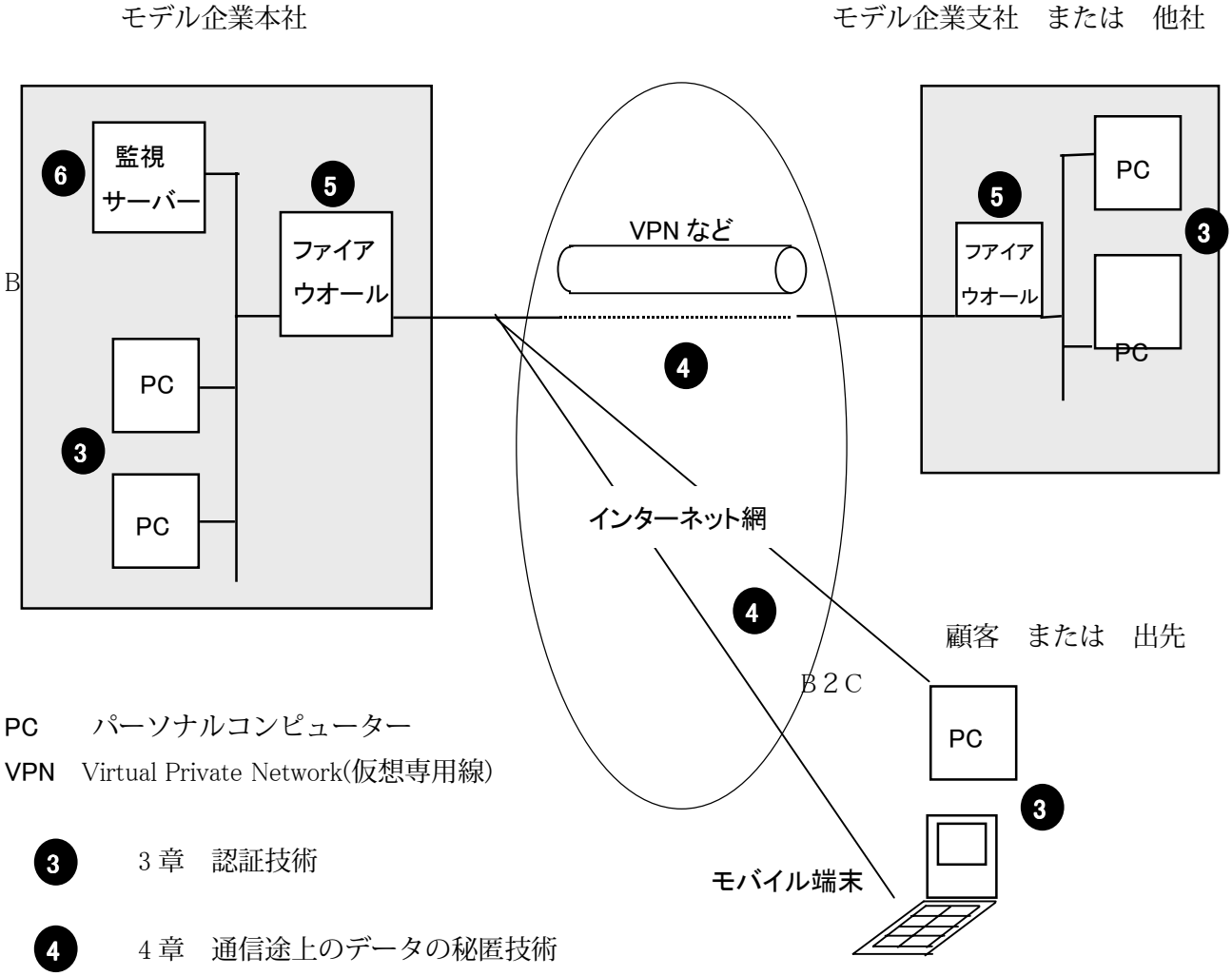
第 4 章は、ネットワーク上に流れる情報が傍受されたり、改ざんされたりしないようにする暗号化の技術についての解説である。暗号化技術は非常に奥が深く世界中で今も盛んに研究が続けられている分野であるが、ここでは、一般の企業が標準的に用いるべき暗号化技術にしぼり製品や技術を解説する。

第 5 章は、各企業のインターネットの入り口にあたるセキュリティ、いわゆるファイアウォールにおける技術をまとめてある。インターネットは公道であり悪意やいたずらの侵入を防ぐこうしたシステムの導入は今や常識となっているが、多くの製品が市場に登場し選択が難しい。 ここでは選択の指針になるような解説を心がけた。

第 6 章は、外部だけでなく、内部のセキュリティ破りにも備えるネットワーク監視技術についての紹介である。ネットワーク内のデータの流れを監視し、不正アクセスを未然に防止する運用技術は今後ますます重要となる。

以上、簡単に各章の内容について概要を述べた。

図２－１　ネットワーク構成図



PC　　パーソナルコンピューター

VPN　Virtual Private Network(仮想専用線)

3　3 章　認証技術

4　4 章　通信途上のデータの秘匿技術

5　5 章　ファイアウオール技術

6　6 章　不正アクセス監視技術

第３章　認証技術

3.1　PKI（公開鍵暗号インフラ）を利用し、通信相手を特定する

(1) PKI とは

PKI（Public Key Infrastructure の略）は公開鍵暗号方式という暗号技術を利用したセキュリティ・インフラである。

(2) PKI 個人認証

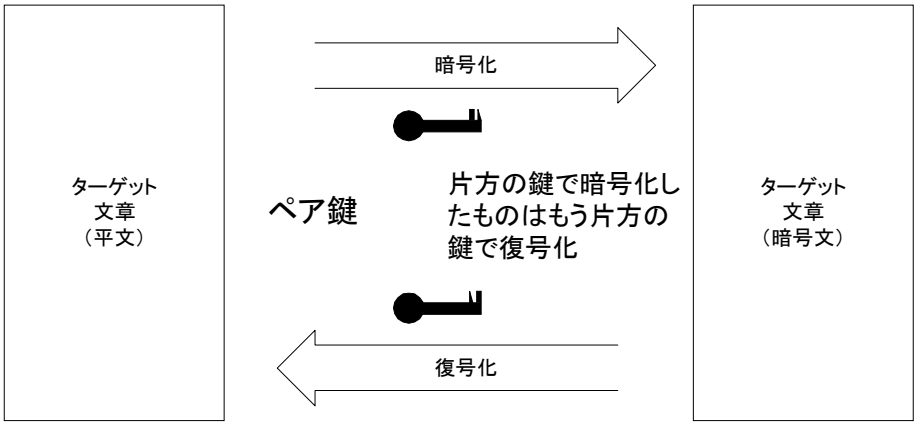
1) PKI 個人認証のキーワード

顔の見えない通信相手を信頼するために防止しなければならない次の４つの行為が PKI のキーワードである。それは、「盗聴」・「改ざん」・「なりすまし」・「否認」である。

2)PKI 個人認証の仕組み

PKI は「片方の鍵で暗号化したものはペア鍵を利用しないと復号できない」という機能を利用する。暗号化に利用した鍵で暗号化したものを復号することはできない。このとき、ペア鍵を秘密鍵（自分のみが知る鍵）と公開鍵（誰でも入手できる鍵）に分けて利用する。

図３－１　PKI



3）文書を暗号化して「盗聴」を防止する

PKI では暗号文書を送信したい人が暗号文書を受け取る人の公開鍵を入手して、暗号化し送付する。受け取った人は秘密鍵を利用して暗号文書を復号する。復号できれば、自分が公開した公開鍵で暗号化されたことが保証される。また、暗号化されているのでデータを見ても中身はわからない。また、公開鍵で暗号化されたものは公開鍵では復号できないので安全である。

4) PKI での電子署名の原理

PKI ではペア鍵の機能を利用して電子署名を実現している。文書を送信する人は文書の平文とその文書を自分の秘密鍵で暗号化したものを一緒に送付する。受け取った人は暗号文書を公開鍵で復号化して、平文と一致すれば、送付した人物を信頼することができる。公開鍵で復号できる暗号は秘密鍵でのみ可能だからである。

5) PKI での電子署名の実際

PKI では実際にはハッシュ関数というものを利用し、電子署名を実現している。

・送信する側の処理（図３－２）

・受信する側の処理（図３－３）

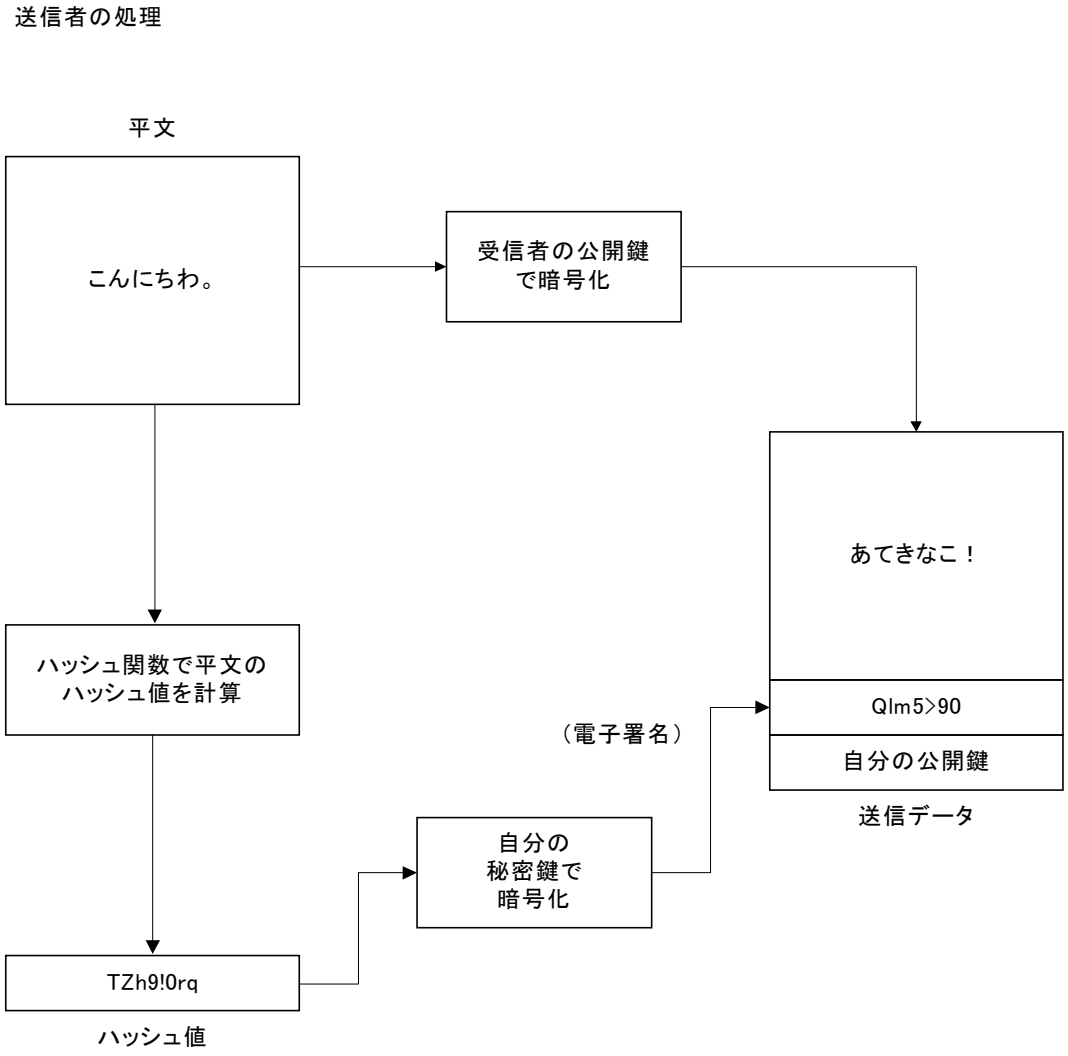
●送信する側の処理

・送信する平文のハッシュ値を計算する。

・作成したハッシュ値を自分の秘密鍵で暗号化し、電子署名とする。（自分が作成した証拠となる）

・平文と電子署名をペアで相手に送信する。

図３－２　送信処理手順



●受信する側の処理

・相手の公開鍵を入手する。

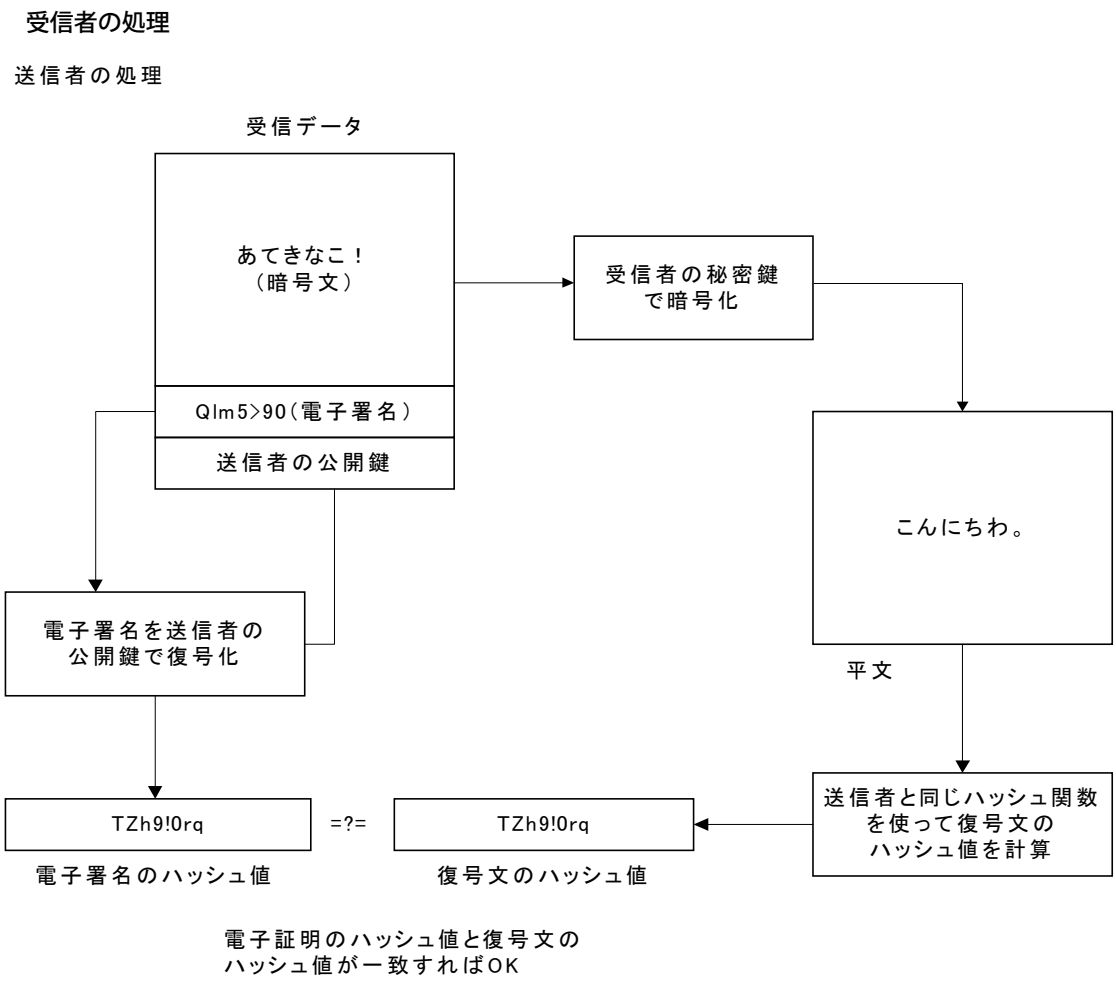
・送信されてきた電子署名を入手した公開鍵で復号化する。

・送信されてきた平文から相手と同じアルゴリズムを用いてハッシュを作成する。

・復号したハッシュと自分が作成したハッシュを比較する。

この値が一致すれば、送信者が署名してから受信者が検証するまでの間に文書が改ざんされていないことになる。また、秘密鍵を利用することで「なりすまし」を防止するとともに、「否認」を回避することができる。

図３－３　受信処理手順



6) 公 開鍵と電子証明書

公開鍵は誰でも入手することが可能であるため、その公開鍵の持ち主を特定する必要がでてくる。それを実現するのが、認証局（CA 局）であり「電子証明書」である。公開鍵を受け取ったら、その鍵の電子証明書の内容を確認し、電子証明書を発行している認証局が信頼できる認証局かどうか確認する必要がある。

（注）ハッシュ関数とは次のような特徴を持つアルゴリズムである。

・元データの長さに関係なくハッシュアリゴリズムによって 128 ビットや 160 ビットの決められた出力値となる。

・元データが変更されれば、ハッシュ値も変化する。

・ハッシュ値から元データに復号することは不可能。

7) PKI を実現するための製品群について

PKI を実現するための製品例である。他のメーカーにも製品がある。導入の目安となるように価格の公表されているものを掲載する。

メーカー名	製品名	対応 OS	価格
日本電気 (注 1)	PKI サーバー/Carassuit Ver2.0(基本 500 ユーザー)	Windows NT Server 4.0 SP5	￥2,000,000
	PKI サーバー/Carassuit Ver2.0(追加 1000 ユーザー)	Windows NT Server 4.0 SP5	￥800,000
	PKI サーバー/Carassuit Ver2.0(無制限ユーザー)	Windows NT Server 4.0 SP5	￥10,000,000
	PKI サーバー/Carassuit Web 申請サービスオプション Ver1.0	Windows NT Server 4.0 SP5	￥800,000
	PKI サーバー/Carassuit CK-Guard オプション Ver1.0	Windows NT Server 4.0 SP5	￥500,000
	PKI サーバー/Carassuit JCSI オプション Ver1.0	Windows NT Server 4.0 SP5	￥500,000
	PKI サーバー/Carassuit ベリサインオプション Ver1.0	Windows NT Server 4.0 SP5	￥500,000

日立製作所 (注２)	PKI Management Program	Windows NT4.0	¥2,000,000
	Enterprise Certificate Server	Windows NT4.0, Windows 2000	¥2,000,000
	PKI Runtime Library	Windows NT4.0, Windows 2000,98,95	¥24,000
	PKI Developer's Toolkit	Windows NT4.0, Windows 2000,98,95	¥2,000,000

(注１)
対応機種 Express5800/100 シリーズ

○必要なソフト
Carassuit RA を利用するために
Microsoft InternetInformationServer Version4 (OptionPack 4)
Oracle8 サーバー、またはクライアント (r8.0.4, r8.0.5)
Netscape Communicator 4.x

○Carassuit CA を利用するために
Oracle8 サーバー、またはクライアント (r8.0.4, r8.0.5)
Netscape Communicator 4.x
SecureWare/IC カード発行キット Ver2.2
IC カードマネージャランタイムライブラリ(RTL)
(注：この RTL は、PKI サーバー/Carassuit に同梱されている)

(注２)
PKI Management Program は、証明書発行ライセンス 100 枚を含む。
100 枚を超える証明書発行には別途ライセンスの購入が必要になる。

(3) SSL

1) SSLとは

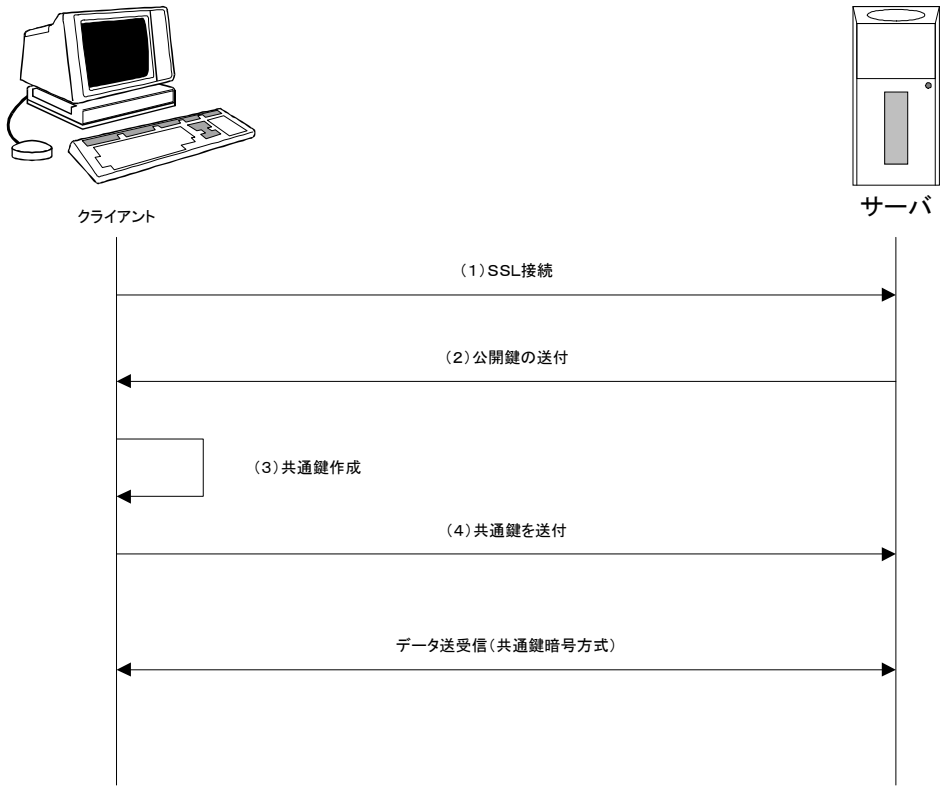
SSL（Secure Socket Layer）は Netscape Communication 社が提唱したプロトコルで、暗号化技術を用いてインターネット通信を安全に行うことを目的としている。SSL 自体の定義は Web 上での利用に限定されたものではないが、現在では Web 上での認証と通信データの暗号化に最も多く利用されている。

2) SSLの仕組み

SSL は公開鍵暗号方式と共通鍵暗号方式の両方を用いて効率的な通信データの暗号化を実現している。公開鍵ペアを利用し、共通鍵の暗号化を行って通信を行い、実際のデータ通信には共通鍵で暗号化を行っている。それは公開鍵での暗号化は共通鍵での暗号化より処理に時間を要するためで、共通鍵を利用し通信時間の短縮を行っている。

SSL での認証方式は一般的にサーバー側が証明書をクライアントに提示し、クライアントは証明書が信頼できる証明機関が発行したものかを確認し、信頼できる場合に通信を継続する。

図３－４　SSLハンドシェイク図



3) SSL の暗号通信手順

・クライアントはサーバーに対し SSL 接続を行う。
・サーバーは認証機関（CA）の秘密鍵で鍵をかけられたサーバー公開鍵を送信する。
・クライアントは認証機関の公開鍵を用いてサーバーが送付してきた公開鍵を復号化する。
・クライアントは共通暗号鍵を作成し、サーバーの公開鍵を用いて暗号化し、サーバーに送付する。
・サーバーはクライントから受け取った公開鍵を自分の秘密鍵で復号化する。
・以降のクライアントとサーバーの通信は共通鍵を用いて行う。

4) SSL の実現する電子証明書サービス

SSL を実現するためのサービス例である。他のメーカーにもサービスがある。導入の目安となるように代表的なものを掲載する。

会社名	サービス名	期間	価格
日本ボルチモア	SureServer for SSL	1 年間	￥ 75,000
日本ベリサイン	セキュア・サーバーID	1 年間	￥ 81,000
	グローバル・サーバーID	1 年間	￥138,000
日本認証サービス	SecureSign サーバーサービス	1 年間	￥ 78,000

●参考文献

日経ネットワーク 2000 年 10 月号
＠IT ホームページ http://www.atmarkit.co.jp/
日立製作所株式会社ホームページ http://www.hitachi.co.jp/
日本電気株式会社ホームページ http://www.sw.nec.co.jp/
日本ボルチモアテクノロジー株式会社ホームページ
http://www.baltimore.co.jp/index.asp
日本ベリサイン株式会社ホームページ http://www.verisign.co.jp/
日本認証サービス株式会社ホームページ http://www.jcsinc.co.jp/

３．２　個人認証の技術

コンピュータシステムの使用者が本人であることの確認は、本人が記憶したパスワードによる方法が古くより行われており、現在でも最も一般的である。しかしながら、パスワードの類推や通信経路の盗聴等によって第三者になりすますことが容易にでき、インターネット時代の認証としては非常に危険である。

本節では、パスワードの盗聴他を防ぐ技術（(1)ワンタイムパスワード）、パスワードに代えて本人の身体的特徴で認証する技術（(2)生体認証）、本人の持ち物により認証する技術（(3) IC カードによる認証）について紹介する。いずれの技術にも弱点はあり、これを補うためには複数の方式を組み合わせることが必要である（多要素認証）。

(1) ワンタイムパスワード

固定パスワードは盗聴やリプレイアタックにより解読され、第三者に不正使用される危険性が大きい。ワンタイムパスワードは毎回異なるパスワードを使用し、これに対抗する。

1) パスワード生成機（トークン）の種類

利用者は、「トークン」により生成されたパスワードをワンタイムパスワードとして使用する。トークンごとに異なる「シーズ」（パスワードを生成する鍵）が格納されている。トークンを第三者に不正使用されることを避けるため、PIN コード（暗証番号）と組み合わせて使用する。

a) ハードトークン

生成したパスワードを表示する窓をもち、カード型、キーホルダー型等の形態がある。トークン携帯者以外は使用できないため安全性が高い。クライアントに特別なモジュールをインストールする必要がなく、PDA や携帯電話等 PC 以外の環境でも利用可能である。電卓のようなキーパッドを備えるタイプのトークンは PIN コードを含めてパスワード化するため、通信経路に PIN コードが流れず、さらに安全性が高い。

b) ソフトトークン

トークンの機能をソフトウエアとして PC にインストールして利用する。トークンの携帯が不要であるため便利であるが、不正使用の危険性は大きくなる。シーズを IC カードに格納し、安全性を高めた製品もある。単にパスワードを生成するだけでなくアプリケーションと連携することが可能である。

2) パスワード生成の方式

a) チャレンジ・レスポンス方式

サーバーがランダムなチャレンジコードを提示し、クライアントがこれに対応したコードを応答することでサーバーがクライアントの認証を行う。チャレンジコードをトークン

に入力するという手間がかかるため利便性に劣る。

b) 時刻同期方式

時刻をもとにパスワードを生成し、一定間隔（30～60 秒）で更新される。サーバー・クライアントの両者で時刻が同期している必要がある。時刻差を補正する機構を備えるため実用上問題は小さいが、万が一、サーバーの時計が大きく狂うと混乱する可能性がある。パスワード更新に一定時間を要するため、連続して認証を受ける必要がある場合は適さない。

c) カウンタ同期方式

アクセスカウンタ値をもとにパスワードを生成する。事前に生成したパスワードを利用できるためこれを書きとめておく等、必ずしもトークンを携帯しなくても利用可能であり、不正使用の機会が生じる。

3) シ ステムへの適用

ワンタイムパスワード製品は、「トークン」と「認証サーバー」から構成される。システムへの適用は、各システムの認証を認証サーバーに対応させることがポイントとなる。ファイアウォール製品、RAS 製品、VPN 製品は、代表的なワンタイムパスワード製品の認証サーバーに対応するものが多い。ユーザー開発のシステムの場合は提供されるツールキットを用いて対応させることができる。

4) 製 品（表３－１）

表 3−1

SecurID、ACE/Server	
開発・販売	RSAセキュリティ(株)　http:// www.rsasecurity. co.jp
方式	時刻同期方式(60秒毎)
ハードトークン	カード型、キーホルダ型、ピンパッド スマートカード(ソフトトークンのシーズの格納)
ソフトトークン	Windows95/98、NT4.0、Palm
費用	ハードトークン：¥9,000/枚～(有効期間２年)、ソフトトークン：¥4,000/ユーザー 認証サーバー(ACE/Server　100 ユーザー例)：¥1,800,000(ﾗｲｾﾝｽ)、¥324,000(年間保守)
備考	ハードトークンの有効期間は最長４年
SAFEWORD	

開発・販売	(株) メトロ　http:// www.tokyo.metro.co.jp
方式	カウンタ同期方式 or チャレンジ・レスポンス方式 (トークン毎に選択可)
ハードトークン	カード型、キーホルダ型、キーパッド(電池交換可タイプ有)
ソフトトークン	Windows3.1/95/98、NT3.41/4.0、SunOS、MacOS、Zaurus、Palm
費用	ハードトークン：¥7,600/枚～(電池寿命３年)、ソフトトークン：¥4,000/ユーザー 認証サーバー(100 ユーザー例)：¥1,500,000(ﾗｲｾﾝｽ)、¥225,000(年間保守)
備考	携帯電話(i モード) をトークンとして用いる「Virrual Token」有

Digipass、VACMan	
開発・販売	(株) ヒューコム　http:// www.hucom.co.jp
方式	時刻同期方式(36秒毎) or チャレンジ・レスポンス方式 (トークン毎に選択可)
ハードトークン	電卓型、光学式(CRTに表示されたチャレンジコードを、トークンが読み取る)
ソフトトークン	なし
費用	ハードトークン：¥10,000/個～(電池交換可) 認証サーバー(VACMan 100 ユーザー例)：¥450,000(ﾗｲｾﾝｽ)、¥81,000(年間保守)
備考	他製品のトークンと比べ大きく、携帯に難あり

ActivCard One	
開発・販売	アクティブカード(株)　http:// www.activcard.com
方式	カウンタ同期方式 or チャレンジ・レスポンス方式 (トークン毎に選択可)
ハードトークン	キーパッド(電池寿命８年、交換可) 、スマートカード
ソフトトークン	なし
費用	
備考	

SecureTicket	
開発・販売	(株) ワイ・ディ・シー　http:// wwwydc. co.j p
方式	FDや HD,メモリーカード等、書き込み可能な媒体をトークンとして使用する。認証の度に次回のパスワードがサーバーより伝達され、トークンに更新格納。クライアントソフトはアプレットで、認証に際しダウンロードされる。
費用	¥500,000(500ユーザー) ～¥6,000,000(無制限ライセンス)
備考	ブラウザ利用時の認証のみ可。

(2) 生体認証（バイオメトリックスによる認証）

生体認証は、指紋、声紋、筆跡、網膜、虹彩等を計測し、正当な本人固有の特徴と合致するかどうかを確認することによって認証する方法である。本人の所有物や知識による認証が盗難や漏洩による「なりすまし」の可能性があるのに対し、その危険が小さい。一方で、あらかじめ登録された情報と完全に一致することはあり得ず、どの程度似ているかという統計的な取り扱いが必要となるため、「本人を本人と認識しない誤り」「他人を本人と認識してしまう誤り」をゼロとすることは難しい。また、プライバシー面（指紋）や、赤外線照射（網膜、虹彩）に対する抵抗感、時間的な変化（声紋、筆跡）等、生体認証ならではの課題も多い。

1) 生 体認証の種類と特徴（表３－２）

表３－２

	特徴	課題	費用
・終生・終生不変	・犯罪捜査を連想するものとして抵抗感が強い ・衛生面の確保	1 万円～	
網膜・虹彩	・終生不変 ・コピーが困難 ・精度は極めて高いとされる	・目に赤外線を照射することに対する抵抗感	30万円～
声紋	・非接触 ・心理的抵抗が少ない	・時間的な変化 ・体調による変化 ・ノイズ等、環境の影響	30万円～
筆跡	・心理的抵抗が少ない ・筆順、筆速、筆圧等も測定	・時間的な変化 ・その時々の変化	
顔	・非接触 ・心理的な抵抗が少ない	・時間的な変化 ・ひげ、メガネ等の影響	

2) 生 体情報の管理と照合

生体情報はそのままのイメージで扱われるわけではなく、個人を識別するための特徴データとして登録、照合される。例えば指紋のイメージデータは数 KB になるが、特徴データは数百 B 程度である。

この生体情報を装置内で管理・照合する方式と、外部（装置を接続した PC やサーバー）で行う方式とがある。一般に装置内で管理・照合する方式の方が生体情報が外部を流れないため安全であるが、外部方式も暗号化等の対策により安全性の高い製品も登場している。

3) シ ステムへの適用

近年、指紋を用いた認証について安価で小型の製品が登場しており、現実的な選択肢となってきた。多くの製品で、Windows やネットワークへのログオン時に指紋認証を行う機能が提供されている。その他のシステムに適用する場合は、SDK を用いて開発する必要がある。

4) 製 品（PCで、指紋認証を実現する製品）（表３－３）

表３－３

SecuDesktop	
開発・販売	日本セキュアジェネレーション(株)　http:/ /wwwsecugen.co.jp
照合方式	PC内で照合
機能	Windowsログオン、画面ロック
装置	EyeDマウス (マウス型、パラレル) 、EyeDキーボード (キーボード型、パラレル) EyeDハムスター (卓上型、USB)
費用	
備考	ファイルの暗号・復号機能有

FIU-710（装置）	
開発・販売	(株) ソニー　http:/ /www.sony.co.jp
照合方式	装置内で照合(最大登録数：1,000 指) を行い、装置－システム間は PKI を用いて認証
機能	(要 アプリ開発)
装置	FIU-710 (薄型、USB)
費用	
備考	

指パス Ver2.0	
開発・販売	オムロン(株)　http://www.omron.co.jp
照合方式	装置で読取った指紋イメージを、PC内で特徴データ化し登録データと照合
機能	Windowsログオン、ネットワークログオン、画面ロック Notes・RAS他各種Windowsアプリケーションのパスワード入力代行
装置	FPS-1000S(卓上型、USB)、FPS-300S(小型、USB)
費用	¥14,800（装置×1、ライセンス×1）
備考	

Fingsensor	
開発・販売	富士通(株)　http://www.fmworld.net
照合方式	装置内で指紋イメージを特徴データ化し、PC内で登録データと照合
機能	Windowsログオン、画面ロック
装置	FS-200P(小型、パラレル)、FS-200U(小型、USB)
費用	¥29,800(装置×1、ライセンス×1)
備考	

Fsas指紋認証システム SF2000V3	
開発・販売	富士通サポート&サービス(株)　http://www.fsas.co.jp
照合方式	装置で読取った指紋イメージを、クライアントPCで暗号データ化、サーバーで照合。 サーバーによる大規模指紋データ管理が可能(1,000～10,000ユーザー)
機能	WindowsNTログオン、Notesログオン
装置	富士通(株) FS-200P/FS-200U、日本電気(株) PK-FP001/PK-FP002 オムロン(株) FPS-1000S、他
費用	¥3,234,000（クライアント×25、装置×25、導入費込の例）
備考	暗号・複合化機能(オプション)

SecureFinger	
開発・販売	日本電気(株)　http://www.sw.nec.co.jp
照合方式	装置内照合(最大登録5指×200人)、PC内照合、サーバー照合(オプション)を選択可能
機能	PC起動、Windowsログオン、画面ロック アプリケーションパスワード代行(Notes、IE、RAS、MS-Office他)
装置	PK-FP001M(PCカード型/PCMCIA)、PK-FP002M(小型/シリアル接続) N7950-41(卓上型/シリアル接続/光学式読取) VersaPro VA50H/SY(指紋センサー内蔵ノートPC)
費用	PK-FP001M：¥44,800、PK-FP002M：¥34,800、N7950-41：¥53,800
備考	

FPR-DTMKII（装置）	
開発・販売	三菱電機(株)　http://fpr.mitsubishi-fpr.com/jp
照合方式	装置内照合(最大登録1,000指)、装置外照合のいずれも可
機能	Windowsログオン(別売)
装置	FPR-DTMKII（小型/パラレル)
費用	
備考	

WinSafe	
開発・販売	システムニーズ(株)　http://www.systemneeds.co.jp
照合方式	IC カードを用いた認証との組み合わせ可
機能	PC起動、Windowsログオン、Windowsネットワークログオン、NDSログオン RASログオン、画面ロック、Notes ログオン
装置	(株) ソニー FIU710
費用	¥190,000(装置×5台、ライセンス×5)
備考	

(3) IC カードによる認証

IC カードはプラスチック製のカードに IC チップを埋め込んだもので、欧米ではスマートカードと呼ばれている。携帯性、安全性に優れていることから、「所有物による本人の認証」に用いられる。

1) IC カードの特徴

a) IC カードの種類

IC カードと IC カードリーダー間ではデータ信号のやりとりが行われる。また IC カード自体には基本的には電池は内蔵しておらず IC カードリーダーから電力の供給が行われる。

インタフェースとして金属端子を接触させる「接触型」と、電磁波を手段とする「非接触型」に分類される。さらに非接触型はリーダー・ライター間距離により、密着型、近接型（～10cm)、近傍型（～70cm)、遠隔型（70cm～）に規格化されている。

また演算機能のために CPU を搭載するもの（CPU 付カード）と、ロジック回路で演算するもの（ワイヤードロジックカード）とがあり、CPU 付カードの方が高度な演算を実現できる。

非接触型 IC カードはカードリーダーに挿入する必要がないため利用者にとって使い勝手

が良い。さらに接点がないためカードリーダーのメンテナンスが大幅に軽減され、カードの接点磨耗、汚れ、静電気等のトラブルを回避できる。一方、電磁波によるため給電量に制約がありCPUは搭載できない。また規格上遠隔型になる程高速で通信できる一方、情報量は少なくなる。

b) IC カードの安全性

IC カードは攻撃に対抗する物理的・論理的セキュリティ機能を備えており、IC カード内に格納された情報を保護することができる。

・IC チップ表面の特殊加工、読み取りが難しいメモリの採用、偽造・変造・改ざんを試みるとダミー回路によりチップそのものが回路的に破壊される等、物理的に保護できる
・アクセス権の設定により、不正アクセスを論理的に防止できる
・カード外部とデータをやり取りする際、これを暗号化することができる
・カードと外部接続装置間で相互に正当であることを認証できる

c) 標準化動向

物理的レベル、電気的レベル、データリンクプロトコルレベルについては、ISO/IEC にて標準化され相互運用が可能となっている（非接触型は、精度の問題等もあり、同一メーカー以外のカードとリーダーの組み合わせでは読み取り自体が困難であることも多い)。しかしアプリケーションレベルではさまざまな仕様が存在するため、アプリケーションごとにこれに対応した IC カードを用いる必要がある。PC（Windows）については Microsoft 社を中心にまとめられた PC/SC（Personal Compurte / Smart Card）仕様を多くのアプリケーションが採用し始めており、主流となりつつある。

2) IC カードを用いた認証

IC カードは携帯が用意であること、安全性が高いことから、「持ち物による本人認証」として用いられる。アプリケーションのユーザーID／パスワードを IC カード内に格納する方式の他、PKI の秘密鍵の格納、ワンタイムパスワードのトークン機能をもつもの等がある。

システムへの LOGIN には接触型 IC カードとするのが一般的であるが、入退室管理にはその利便性・保守性のため非接触型が採用される傾向にある。これを 1 枚のカードで実現するため、両者を一体とした「ハイブリッドカード」がある。

3) シ ステムへの適用

a) ID／パスワード格納方式

利用するシステムのユーザーID とパスワードを IC カードに格納し、PC に導入したソフトウエアでこれを読み出しシステムへ渡して認証を行う（このパスワードは利用者は意識しない)。 推測しにくいパスワードを設定することにより、IC カードを保有していないと事実上利用できない。

・特徴

◎システム側で特別な対応は不要であり、導入が容易。

×通信経路の盗聴やリプレイアタックに対しては対抗できない（システムに依存）

×パスワード変更の度に IC カードの書き換えが必要であるため、定期的な変更は困難

b) PKI 秘密鍵格納方式

PKI の秘密鍵を IC カードに格納し、PKI の弱点となる秘密鍵管理を確実にする。単に鍵を格納するのみではなく、データの暗号復号を IC カード内で処理することにより鍵情報の漏洩を防ぐ。

・特徴

◎IC カードの盗難や不正使用以外のあらゆる脅威に対抗できる

△PKI 導入が前提であり、運営を含め大規模な対応を要する

c) ワンタイムパスワード方式

ワンタイムパスワードのトークン機能を IC カードにもち、PC に導入したソフトウエアを介してワンタイムパスワードに対応したシステムへの認証を行う。ワンタイムパスワードそのものを利用者がタイピングする必要がなく、ワンタイムパスワードの欠点である利便性が改善される。シーズを IC カード内に格納するのみではなく、トークン機能そのものを IC カードにもちシーズ情報の漏洩を防ぐ製品もある。

・特徴

○安全性に優れる

※ワンタイムパスワードの導入が前提となる

4) 製 品（PCで、ICカード認証を実現する製品）（表３－４）

表３－４

WinSafe	
開発・販売	システムニーズ(株)　http://www.systemneeds.co.jp
方式	ID/パスワード格納
機能	PC起動、Windowsログオン、Windows ネットワークログオン、NDS ログオン RASログオン、画面ロック、Notes ログオン
費用	IC カード：　¥9,800～(ライセンス付)、¥5,000～(再発行用) リーダライタ：　¥8,000(シリアル接続型)、¥17,000(PCMCIA 型)
備考	ファイルの暗号・復号機能有、指紋照合との組み合わせ可

ARCACAVIS	
開発・販売	(株) ネット・タイム　http://www.nettime.co.jp
方式	ID/パスワード格納
機能	WindowsNTログオン、RASログオン、画面ロック、Notesログオン
費用	ICカード：　¥2,000 ライセンス：　¥16,000(NT)、¥8,000(RAS)、¥16,000(ロック)、¥14,000(Notes) リーダライタ：　¥12,000(シリアル接続型)、¥25,000(PCMCIA型)
備考	ファイルの暗号・復号機能(オプション) SecureIDソフトトークンのシーズを格納可 PKI鍵・証明書の格納可

ActivCard Gold	
開発・販売	アクティブカード(株)　http://www.activcard.com
方式	ID/パスワード格納(最大10) ワンタイムパスワード(ActivCard One)
機能	Windowsログオン、NDSログオン、RASログオン
費用	
備考	PKI鍵・証明書の格納および署名・復号機能の搭載可(Entrust、Baltimore)

Windows2000	
開発・販売	マイクロソフト(株)　http://www.microsoft.com/japan
方式	PKI
機能	Windowsネットワークログオン、画面ロック
費用	（Windows2000に含まれる）
備考	Gemplus社、Schlumberger社のICカード用ドライバ添付 ホワイトペーパー(スマートカードを使ったログオン方法)： www.microsoft.com/ japan/windows2000/library/howitworks/security/sclogonwp.asp)

● 参考文献

・バイオメトリックスによる個人認証技術の現状と課題（日本銀行金融研究所／金融研究／2000.4）
・IC カードシステム利用促進協議会ホームページ（http://www.jicsap.com）
・IC カード対応セキュリティーシステム推進協議会ホームページ（http://www.ssipg.gr.jp）
・大日本印刷(株)ホームページ／テクニカルレポート（http://www.dnp.co.jp/bf/tech）
・本文掲載各社のホームページ

第４章　通信途上のデータの秘匿

4.1　拠点間通信に用いられる回線

(1) 専用線

従来、社内 LAN と同等のセキュリティと通信品質が求められる企業等の拠点間通信の構築には、第三者による伝送中の盗聴や LAN への不正アクセスを防ぐことができ、通信品質（通信速度）は常に一定に保たれていることから、専用線が使用されてきた。しかし、一対の拠点間接続に 1 本の専用線が必要であり、拠点数の増加に伴い回線数も増加するため、拠点間通信を構築するためには高いコストが必要であった。

(2) フレームリレー

専用線の短所を補ったのがフレームリレーである。フレームリレーは通信事業者が提供するフレームリレーサービスを利用するもので、拠点のネットワークをフレームリレー網に接続することで企業内通信網を構築することが可能になった。フレームリレーサービスは専用線とは違い一般回線を利用したものであるが、その基盤をサービス提供者が提供しメンテナンスするため第三者による不正利用が不可能であり、フレームリレー利用者が通信回線を共有するため通信品質が低下する恐れがあるが、高い通信品質を保証する契約を選択することにより回避は可能である。

(3) IP-VPN

現在、フレームリレーの後継として IP-VPN が登場している（VPN：Virtual Private Network）。IP-VPN とはフレームリレーと同様に通信事業者が保有するネットワークを使用したサービスである。フレームリレーとの相違点は通信料金と通信品質にある。通信料金においては、フレームリレーは接続する拠点間の距離が長くなるにしたがって通信料金が増加するが、IP-VPN では拠点間の距離に通信料金が影響されないサービスである。ただし、拠点間の距離が短い場合、フレームリレーの方が安価な場合があるため注意が必要である。また、IP-VPN を利用するにあたり、LAN 側に特別な装置は必要なく通常しているルーターをそのまま使用している点でもコストの抑制を実現できる。しかし、IP-VPN サービスを提供する通信業者は他の通信業者のネットワークと相互接続せず、自己完結したネットワークによりサービスを提供しているため、各拠点で同一の通信業者からサービスを受ける必要がある。また、通信品質においては、通信網内のデータをほとんど遅延なしに高速に伝送するため、高速な拠点間通信網を実現することができる。

IP-VPN を提供する通信業者の主だったものには以下がある（表４－１）。

表４－１

名称	開発元	鍵長	特徴
DES	ＩＢM社	56bit	米国政府が標準暗号化方式として採用
トリプル DES		112bit 相当	二つの鍵を使って DES の処理を 3 回行う。
IDEA	Ascom Tech 社	128bit	DES より処理が高速な上暗合強度が強い。開発後の時間が短く十分な安全性が未確認。
FEAL	ＮＴＴ	64bit	暗合強度の改良により、現在は FEAL-32 が使用されている。
RC2 および RC4	ＲＳＡ ｾｷｭﾘﾃｨ社	可変	鍵の長さを変えることができる。

(4) VPN（インターネット VPN）

通信業者の提供する公衆回線網を使用したサービスである IP-VPN とは別に、通信業者を介さずにインターネットを利用して仮想的なプライベートネットワークを実現する技術に VPN がある。これは IP-VPN と区別するためにインターネット VPN とも呼ばれるが、ここでは VPN と表記する。

VPN により拠点間通信を実現するためには LAN とインターネットとの接続点に VPN 装置を設置する必要がある。VPN 装置には VPN 機能を単独で実現した機器あるいは VPN 機能が組み込まれたファイアウォール製品やルーター製品がある。それらの製品はトンネリング技術を用いることにより仮想的なプライベートネットワークを実現している。トンネリングとは LAN から送出されるデータを VPN 装置がカプセル化し、そのカプセル化されたデータを受信した VPN 装置はカプセル化を解除することにより本来のデータを受信側の LAN 上に送り出す技術である。また、送出する TCP/IP パケットを IPSec により暗号化してからカプセル化することで、盗聴や IP アドレスの不正使用からも防ぐことができる。

VPN の長所としては、その拠点間通信に通信業者を利用しないため IP-VPN と比較してランニングコストの点において安価に仮想的なプライベートネットワークを運用することができる。その反面、導入時において、自前でネットワークを構築する必要があるため、その導入および運用に技術力と人的な体力が必要となる。また、VPN ではインターネットを拠点間通信に利用するため拠点内のセキュリティ確保の観点からファイアウォールの設置が必要となる。通信品質については、インターネットを拠点間通信に利用するため、高い通信品質を確保することができないといった短所もある。

4.2　エクストラネットにおけるセキュリティ対策

VPN を用いることにより一般回線を利用したインターネットの通信網を利用して専用線と同じような機密性の高いネットワークの構築が可能である。

VPN は盗聴に対するセキュリティ対策を施すことは可能だが、なりすましによる暗号鍵が不正に使われた場合、誤認する恐れがあるため、信頼できる第三者が管理する公開鍵暗号方式を採用した相互認証が必要になる。

また、通信を行う一方のセキュリティレベルが低い場合、VPN 全体のセキュリティレベルが低いものになるため、VPN を使用して通信を行う双方のセキュリティレベルを高いものにする必要がある。

4.3　データの暗号化

不正な盗聴や窃盗からの情報の保護には暗号処理が効果的である。

暗号処理には市販の暗号化アプリケーションソフトによるものや、それ以外のワープロ、表計算ソフトなどのアプリケーションソフト本体が標準で備えている暗号化機能を利用することもでき、比較的容易に導入することが可能である。

しかし、暗号化処理では暗号化に使用した鍵の管理が難しくなる問題が生じる。特にグループなどでファイルを共有する場合、鍵の保管場所や管理方法などの運用ルールを徹底させる必要がある。

運用ルールの徹底を怠った場合、暗号化したデータの不正な復号が行われたり、暗号データが復号できなくなる問題が発生する恐れがある。

データ通信における暗号化処理には上述のソフトウエアによる暗号化処理の他に専用のハードウエアによる暗号化処理があり、暗号通信機器や暗号処理機能のついたルーター、あるいはファイアウォールの追加機能としてVPN機能を装備することによって情報漏洩を防ぐことができる。

暗号化の方法には公開鍵暗号処理方式と共通鍵暗号処理方式の２種類がある。

4.4　共通鍵暗号方式

共通鍵暗号方式は暗号化とその複合に同一の鍵を使用する暗号方式で、仕様が一般に公開されているため、現在広く使われている暗号方式である。

この方式では暗号化と復号において、同一の鍵を使用する。つまり、送信側は平分を暗合鍵を使って暗号化し、受信側では送信側とが暗号化したものと同じ鍵を用いて復号を行い平文を得る。

その長所は公開鍵暗号方式に比べて暗号処理を高速に行うことができる点にある。しかしその反面、送信側と受信側が同一の暗合鍵を使用するため、暗号化の安全性は暗号化のための鍵を第三者に入手されないことが条件であり、鍵の配送とその管理方法を厳重にしなければならない短所がある。

共通鍵暗号方式の代表的なものには下表のものがある。

表４－２

通信業者名	サービス名	備考
ＫＤＤＩ	IP-VPN サービス（仮称）	既存のフレームリレーをアップグレードする方法と純粋な IP-VPN を提供する２種類のサービスがある。
日本テレコム	ＳＯＬＴＥＲＩＡ	
ＮＴＴ－ＭＥ	ＸｅＰｈｉｏｎ高速ＩＰエクストラネットサービス	
富士通	ビジネス IP ﾈｯﾄﾜｰｸサービス	IP-VPN の先駆けとなったサービス
ＮＴＴコミュニケーションズ ＮＴＴ　ＰＣコミュニケーションズ 日本テレコム	OBN（Open Business Network）	(財)流通システムの開発センターが使用を開発

4.5　公開鍵暗号方式

公開鍵暗号方式は公開鍵と秘密鍵の２つの非対称なデータ暗号化鍵を使用して、暗号化と複合化に別々の鍵を用いる暗号方式である。

この方式では送信者は受信者の公開された鍵で暗号化を行い、受信者は受信者の管理する秘密鍵で復号を行い平文を得る。

共通鍵暗号方式では当事者が鍵を共有するため、同じ鍵を秘密裏に入手しなくてはならないが、公開鍵暗号方式では公開鍵の入手を秘密裏に行う必要がないため、鍵配送を容易に行うことができる。

また、共通鍵暗号方式では通信相手が増えるにしたがって、それぞれの相手と別々の鍵を使って通信をする必要があるため、ｎ人と通信をする場合、全体でｎ（ｎ－１）／２個の鍵が必要だが（ある個人がｎ人と通信を行う場合、その個人は（ｎ－１）個の鍵を管理する必要がある）、公開鍵暗号方式で使用する鍵の個数は２個（公開鍵と秘密鍵）で済むため、鍵の管理が容易になる。

公開鍵暗号方式を共通鍵暗号方式と比較した場合、上述のような長所があるが、その反面、暗号化処理速度が低速であり、長い文書全体を暗号化することには向いていないため、現状では共通鍵と公開鍵暗号方式を組み合わせた処理により、お互いの短所を補った暗号処理が採用されている。つまり、暗号化したい文書全体（データ量多）を共通鍵暗号方式で暗号化し、その共通鍵暗合方式で使用した鍵（データ量少）を共通鍵暗号方式で暗号化する方式である。

公開鍵暗号方式の有名なものにはRSAセキュリティ社が開発したRSA暗合方式がある。

4.6　暗号化製品

暗号化製品の一部を表４－３に挙げる。

●参考文献および出典元

・ネットワークセキュリティ　攻撃と防御のメカニズム　オーム社
・図解　暗合と情報セキュリティ　日経ＢＰ社
・情報処理振興事業協会（ＩＰＡ）ホームページ　http://www.ipa.go.jp/
・インターネットセキュリティがわかる　技術評論社

表４－３

製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
4758-001,013 PCI 暗号化ｺﾌﾟﾛｾｯｻ	IBM	日本 IBM	共通鍵 公開鍵、 署名	DES(56bit) RSA(512,768,1024bit)		暗号化 PCI ﾊﾞｽ・ ｱﾀﾞﾌﾟﾀｶｰﾄﾞ
4758-002,023 PCI 暗号化ｺﾌﾟﾛｾｯｻ	IBM	日本 IBM	共通鍵 公開鍵、 署名	DES(56bit) RSA(512,768,1024,2048bit)		暗号化 PCI ﾊﾞｽ・ ｱﾀﾞﾌﾟﾀｶｰﾄﾞ
AsgentIt!	ｱｽﾞｼﾞｪﾝﾄ	ｱｽﾞｼﾞｪﾝﾄ	共通鍵 公開鍵	DES(56bit) RSA(1024bit)		ﾌｧｲﾙ暗号 ｿﾌﾄｪｱ 無償ﾀﾞｳﾝﾛｰﾄﾞ可
Atalla A10000E NSP	Compaq Computer	ｺﾝﾊﾟｯｸｺﾝﾋﾟｭｰﾀ	共通鍵	DES(56bit)		暗号化ﾌﾟﾛｾｯｻ
Atalla TrustMaster CSP	Compaq Computer	ｺﾝﾊﾟｯｸｺﾝﾋﾟｭｰﾀ	共通鍵 公開鍵、 鍵配送 署名 ﾊｯｼｭ	DES, RC2, RC4(各 40bit) RSA(公開鍵 256～2048bit, 鍵配送 256～512bit) DSA MD2, MD5, SHA-1	FIPS140-1 Level3, UL, CSA, TUV	CryptoAPI 用 暗号化ﾊｰﾄﾞｳｪｱ
BOS	ﾋﾞｰｵｰｴｽ・ﾈｯﾄﾜｰｸ研究所	ﾋﾞｰｵｰｴｽ・ﾈｯﾄﾜｰｸ研究所	共通鍵	TripleDES		暗号、認証、署名ｼｽﾃﾑ
Choas InforGuard v4.02a	国際情報科学研究所	国際情報科学研究所	共通鍵	GCC ｶｵｽ暗号（320bit)		ﾌｧｲﾙ暗号化 ｿﾌﾄｪｱ
CK ガード	NEC	NEC	共通鍵 公開鍵	DES(56bit) RSA（512～4096bit）		秘密鍵装置
CP ロック （パソコン用）	ｼｰｱｲｼｰｼｽﾃﾑｽﾞ （他社と共同）	ｼｰｱｲｼｰｼｽﾃﾑｽﾞ	共通鍵	独自暗号方式(128bit) ・ﾃｷｽﾄ暗号 ・ﾌｧｲﾙ暗号		暗号化ｿﾌﾄｪｱ
CryptoSwift	RAINBOW Technologies	RAINBOW Technologies	公開鍵 鍵配送 署名	RSA(384～1024bit) DSA Diffie-Hellman	SSL, X.509, S/MIME, PKCS, SET, SSH,	暗号 PCI ﾊﾞｽﾎﾞｰﾄﾞ

					IKE, IPSec, TLS, SWAN, FIPS	
D-RANS	KENWOOD ﾛｰﾚﾙｲﾝﾃﾘｼﾞｪﾝﾄｼｽﾃﾑｽﾞ	ﾛｰﾚﾙｲﾝﾃﾘｼﾞｪﾝﾄｼｽﾃﾑｽﾞ	共通鍵 公開鍵 鍵共有	DES, SXAL/MBAL, MISTY, MULTI, FEAL RSA KPS		暗号化ｿﾌﾄｪｱ
Entrust/ICE	Entrust Technologies	ｴﾝﾄﾗｽﾄｼﾞｬﾊﾟﾝ NTT ﾃﾞｰﾀ(SI ﾊﾟｰﾄﾅｰ) ｾｺﾑ情報ｼｽﾃﾑ ｾｺﾑ ｻｲﾊﾞｰｾｷｭﾘﾃｨ事業部 ﾈｯﾄﾏｰｸｽ	共通鍵 公開鍵、 鍵配送 ﾊｯｼｭ	CAST(64,80,128bit), DES, TripleDES, RC2(40,128bit) RSA(1024bit), DSA, Diffie-Hellman SHA-1, MD2, MD5	FIPS140-1 ISO IS15408, CC EAL3 X.509, PKIX PKCS#7, #10, #11	・ Entrust/Entelligence が必要 ・任意のﾌｫﾙﾀﾞをｾｷｭｱ・ﾌｫﾙﾀﾞとして設定し、自動的な暗号化を行う ・削除ﾌｧｲﾙの復旧を防ぐ、完全削除機能(True Delete)をｻﾎﾟｰﾄ ・鍵管理機能により、復号鍵を紛失した場合でも復旧可能
e-Parcel	e-Parcel	東芝情報ｼｽﾃﾑ		SSL		ﾃﾞｰﾀ転送
FastMAP	RAINBOW Technologies	RAINBOW Technologies	公開鍵 鍵配送 署名	RSA(4～4096bit) Diffie-Hellman DSA	IPSec, IKE, ISAKMP, SSL, SET	暗号 LSI
FEAL ・ ESIGN ・ 楕円 DH	NTT ｱﾄﾞﾊﾞﾝｽﾃｸﾉﾛｼﾞ	NTT ｱﾄﾞﾊﾞﾝｽﾃｸﾉﾛｼﾞ	共通鍵 公開鍵 署名	FEAL(128bit) 楕円 DH(256bit) ESIGN(768bit)	ISO/IEC 9979	暗号化ｿﾌﾄｪｱ（関数）
FILE LOCK with FEAL	NTT ｱﾄﾞﾊﾞﾝｽﾃｸﾉﾛｼﾞ	NTT ｱﾄﾞﾊﾞﾝｽﾃｸﾉﾛｼﾞ	共通鍵 公開鍵 署名	FEAL(128bit) 楕円 DH(256bit) ESIGN(768bit)	MOSS	ﾌｫﾙﾀﾞ・ﾌｧｲﾙの暗号化 ｿﾌﾄｪｱ
F-Secure DESktop	F-Secure	山田洋行	共通鍵	TripleDES(168bit), Blowfish(256bit)	-	ﾌｧｲﾙ暗号ｿﾌﾄｪｱ（On-Demand）

F-Secure File Cryipto	F-Secure	山田洋行	共通鍵	TripleDES(168bit), Blowfish(256bit)	-	ﾌｧｲﾙ暗号ｿﾌﾄｪｱ（On-the-Fly）
F-Secure SSH2 /Server for UNIX /Client for Windows, Macintosh, UNIX	F-Secure	山田洋行	共通鍵 公開鍵	TripleDES(168bit), ｵﾌﾟｼｮﾝ (IDEA(128bit)), Blowfish(128bit), Twofish(128), ARC4(128bit) DSA(512-1024bit）, RSA(512-4096bit)	SSH2	ｿﾌﾄｪｱ
IKEVIEW	松下電工	松下電工	共通鍵	DES(40,56bit), TripleDES(112,168bit）	IPsec ISAKMP /Oakley	ﾘｱﾙﾀｲﾑ IPSec, ISAKMP 解析 ｿﾌﾄｪｱ
InstaGate	Technologic	Technologic	共通鍵 ﾊｯｼｭ	DES(56bit), TripleDES(168bit), RC2(40bit), RC4(40,128bit), Safer(128bit) MD5	ICSA S/WAN	ﾊｰﾄﾞｳｪｱ
Interceptor	Technologic	Technologic	共通鍵 ﾊｯｼｭ	DES(56bit), TripleDES(168bit), RC2(40bit), RC4(40,128bit), Safer(128bit) MD5	ICSA S/WAN	ﾊｰﾄﾞｳｪｱ
KPS Cipher PC Guard	ｱﾄﾞﾊﾞﾝｽ	ｱﾄﾞﾊﾞﾝｽ	共通鍵 鍵共有	DES(56bit) KPS		KPS 対応暗号通信用 PC ｶｰﾄﾞ
KPS CipherPRO	ｱﾄﾞﾊﾞﾝｽ	ｱﾄﾞﾊﾞﾝｽ	共通鍵 鍵共有	DES(56bit) KPS		ﾌｧｲﾙ暗号ｿﾌﾄｪｱ
KPSAGS	ｱﾄﾞﾊﾞﾝｽ	ｱﾄﾞﾊﾞﾝｽ	鍵共有	KPS		KPS 鍵配送方式の ID を生成するｿﾌﾄｪｱ
MELWALL A3000-1	三菱電機	三菱電機	共通鍵	MISTY(128bit)		暗号ｱﾀﾞﾌﾟﾀ ﾊｰﾄﾞｳｪｱ
MELWALL H3000-1	三菱電機	三菱電機	共通鍵	MISTY(128bit)		集線型暗号装置 ﾊｰﾄﾞｳｪｱ
MELWALL Mgr	三菱電機	三菱電機	共通鍵 公開鍵	MISTY(128bit) RSA(512bit)		鍵管理ｿﾌﾄｪｱ

MELWALL P3000	三菱電機	三菱電機	共通鍵	MISTY(128bit)		暗号ﾄﾞﾗｲﾊﾞｿﾌﾄｪｱ (WAN 対応)
MELWALL P3000CL	三菱電機	三菱電機	共通鍵	MISTY(128bit)		暗号ﾄﾞﾗｲﾊﾞｿﾌﾄｪｱ (LAN 対応)
MistyGuard/ CRYPTOFILE	三菱電機	三菱電機	共通鍵 公開鍵	MISTY(128bit) RSA(1024bit)		ﾌｧｲﾙ暗号化 ｿﾌﾄｪｱ
MistyGuard/ DIGICAPSULE	三菱電機	三菱電機	共通鍵 公開鍵	MISTY(128bit) RSA(1024bit)	X.509	暗号化ｺﾝﾃﾝﾂ配布
nCipher KeySafe	nCipher	東京ｴﾚｸﾄﾛﾝ	公開鍵 署名 鍵配送	RSA, El Gamal DSA Diffie-Hellman	X.509 SSL v2/v3 TLS PKCS#11	・鍵管理 GUI ｿﾌﾄｪｱ ・K of N による秘密鍵分散管理機能
NE-Secure	ｿﾘﾄﾝｼｽﾃﾑｽﾞ	ｿﾘﾄﾝｼｽﾃﾑｽﾞ	共通鍵 公開鍵	FEAL, DES RSA		LAN間接続の暗号ﾙｰﾀ
NetSwift 1000 PCI Card	RAINBOW Technologies	RAINBOW Technologies	共通鍵 公開鍵 署名 鍵配送 ﾊｯｼｭ	DES(56bit), TripleDES, RC4 RSA(384～1024bit) DSA Diffie-Hellman MD5, SHA-1, HMAC	IPSec DMA ISO	暗号 PCI ｶｰﾄﾞ
nFast PCI Crypto Accelerator	nCipher	東京ｴﾚｸﾄﾛﾝ	公開鍵 署名 鍵配送	RSA DSA Diffie-Hellman	SSL v2/v3 TLS SET S/MIME	・SSL 暗号化ｱｸｾﾗﾚｰﾀ (PCI 接続) ・各種 Web ｻｰﾊﾞ対応 API(MS CryptoAPI、OpenSSL 他対応)
nFast SCSI Crypto Accelerator	nCipher	東京ｴﾚｸﾄﾛﾝ	公開鍵 署名 鍵配送	RSA DSA Diffie-Hellman	SSL v2/v3 TLS SET S/MIME	・SSL 暗号化ｱｸｾﾗﾚｰﾀ (SCSI 接続) ・各種 Web ｻｰﾊﾞ対応 API(MS CryptoAPI、OpenSSL 他対応)
nForce Hardware Security Modules	nCipher	東京ｴﾚｸﾄﾛﾝ	共通鍵 公開鍵 署名	DES(56bit), TripleDES, CAST RSA, El Gamal DSA	SSL v2/v3 TLS SET	・SSL 暗号化ｱｸｾﾗﾚｰﾀ (PCI 接続) ・各種 Web ｻｰﾊﾞ対応 API(PKCS#11、 MS CryptoAPI 、

			鍵配送 ﾊｯｼｭ	Diffie-Hellman MD2, MD5, SHA-1, HMAC	S/MIME PKCS#11	OpenSSL 他対応)
nForce SCSI Hardware Security Modules	nCipher	東京ｴﾚｸﾄﾛﾝ	共通鍵 公開鍵 署名 鍵配送 ﾊｯｼｭ	DES(56bit), TripleDES, CAST RSA, El Gamal DSA Diffie-Hellman MD2, MD5, SHA-1, HMAC	SSL v2/v3 TLS SET S/MIME PKCS#11 FIPS140-1 ﾚﾍﾞﾙ2 認定	・SSL 暗号化ｱｸｾﾗﾚｰﾀ(SCSI 接続) ・ﾊｰﾄﾞｳｪｱｾｷｭﾘﾃｨﾓｼﾞｭｰﾙ(HSM) ・FIPS140-1 ﾚﾍﾞﾙ 2 認定 ・各種 Web ｻｰﾊﾞ/PKI ｱﾌﾟﾘｹｰｼｮﾝ対応 API(PKCS#11、 MS CryptoAPI 、 OpenSSL 他対応)
NLC0099	NTT ｴﾚｸﾄﾛﾆｸｽ	NTT ｴﾚｸﾄﾛﾆｸｽ	公開鍵	最長 2048bit		各種暗号製品
NLC0268	NTT ｴﾚｸﾄﾛﾆｸｽ	NTT ｴﾚｸﾄﾛﾆｸｽ	共通鍵	DES(56bit), TripleDES(112bit,168bit)		各種暗号製品
nShield Hardware Security Modules	nCipher	東京ｴﾚｸﾄﾛﾝ	共通鍵 公開鍵 署名 鍵配送 ﾊｯｼｭ	DES(56bit), TripleDES, CAST RSA, El Gamal DSA Diffie-Hellman MD2, MD5, SHA-1, HMAC	SSL v2/v3 TLS SET S/MIME PKCS#11 FIPS140-1 ﾚﾍﾞﾙ3 認定	・ﾊｰﾄﾞｳｪｱｾｷｭﾘﾃｨﾓｼﾞｭｰﾙ(HSM) ・FIPS140-1 ﾚﾍﾞﾙ 3 認定 ・各種 PKI ｱﾌﾟﾘｹｰｼｮﾝ 対応 API(PKCS#11、 MS CryptoAPI 他対応) ・nCipher KeySafe ｿﾌﾄｪｱによる鍵管理 ・K of N による秘密鍵分散管理機能

NSOC3	RAINBOW Technologies	RAINBOW Technologies	共通鍵 公開鍵 署名 鍵配送	DES(56bit), TripleDES, RC4 RSA DSA, 楕円 DSA Diffie-Hellman, 楕円 Diffie-Hellman	IPSec IKE	暗号 PCI ｶｰﾄﾞ
NX7000 暗号ﾎﾞｰﾄﾞ	NEC	NEC	共通鍵 公開鍵	DES(56bit), TripleDES RSA（512～1024bit）	FIPS140-1	暗号ﾎﾞｰﾄﾞ
Page Vault	Authentica Security	ﾃﾞｨｱｲﾃｨ	共通鍵	RC4(128bit)		暗号化ｿﾌﾄｪｱ
PGP Certificate Server	Network Associates	日本ﾈｯﾄﾜｰｸｱｿｼｴｲﾂ	共通鍵 公開鍵 鍵配送	TripleDES(120 ～ 168bit), IDEA(128bit), CAST(128bit) RSA(最大 2048bit) Diffie-Hellman(最大 4096bit)	PGP	鍵管理ｻｰﾊﾞ ｿﾌﾄｪｱ
PGP for SDK	Network Associates	日本ﾈｯﾄﾜｰｸｱｿｼｴｲﾂ	共通鍵 公開鍵 鍵配送	TripleDES(120 ～ 168bit), IDEA(128bit), CAST(128bit) RSA(最大 2048bit) Diffie-Hellman(最大 4096bit)	PGP	PGP ｼｽﾃﾑ開発 ﾓｼﾞｭｰﾙ
PointSec!	ProtectData	ﾒﾄﾛ NEC ｿﾌﾄ	共通鍵	BlowFish(56,256bit), CAST(56,128bit)	ANSI X9.9	企業向けﾊｰﾄﾞﾃﾞｨｽｸ丸ごと暗号化ｿﾌﾄｪｱ
Private Internet Exchange	Cisco Systems	日本ｼｽｺｼｽﾃﾑｽﾞ	共通鍵	DES(56bit)	NAT	ﾊｰﾄﾞｳｪｱ
Protect Plus	DECROS	東芝情報ｼｽﾃﾑ	共通鍵	WinCros(80 or 160bit), WinCros (80 or 160bit), CAST		ﾌｧｲﾙ暗号化ｿﾌﾄｪｱ
SecureBOX（ｾｷｭｱﾎﾞｯｸｽ）	富士通北陸ｼｽﾃﾑｽﾞ	富士通北陸ｼｽﾃﾑｽﾞ	共通鍵	DES(56bit),TripleDES(168bit),RC2(40,64,128,256bit)	PKCS#5	ﾌｧｲﾙ暗号化／圧縮ｿﾌﾄｪｱ 自動暗号化が可能 管理者による緊急時ﾃﾞｰﾀﾘｶﾊﾞﾘが可能
SECURE PC CARD	富士通ﾋﾞｰ・ｴｽ・ｼｰ	富士通ﾋﾞｰ・ｴｽ・ｼｰ	共通鍵	DES(56bit)		ｾｷｭｱ活性化方式（自動暗号復号） ・指紋認証版 ・ﾊｰﾄﾞｳｪｱ版（PC ｶｰﾄﾞ） ・ｿﾌﾄｪｱ版

SecureExplorer 防人	ﾛｰﾚﾙｲﾝﾃﾘｼﾞｪﾝﾄｼｽﾃﾑｽﾞ	ﾛｰﾚﾙｲﾝﾃﾘｼﾞｪﾝﾄ ｼｽﾃﾑｽﾞ	共通鍵	SXAL/MBAL		暗号化ｿﾌﾄｪｱ
SecureWare/ IC ｶｰﾄﾞ発行ｷｯﾄ	NEC	NEC	公開鍵 ﾊｯｼｭ	RSA（1024bit） MD5,SHA-1		ｿﾌﾄｪｱ
SecureWare/ 暗号ﾎﾞｰﾄﾞﾏﾈｰｼﾞｬ	NEC	NEC	共通鍵 公開鍵	DES(56bit), TripleDES RSA（512～1024bit）		暗号ﾎﾞｰﾄﾞの制御ｿﾌﾄｪｱ
SecureWare/ 秘密鍵ﾏﾈｰｼﾞｬ	NEC	NEC	共通鍵 公開鍵	DES(56bit) RSA（512～4096bit）		秘密鍵管理ｿﾌﾄｪｱ
SecurityPack'98	ｼｽﾃﾑﾆｰｽﾞ	ｼｽﾃﾑﾆｰｽﾞ	共通鍵	ｶｵｽ量子化多値暗号(56bit)		IC ｶｰﾄﾞ対応ｾｷｭﾘﾃｨｼｽﾃﾑ
SmartCipher （ｽﾏｰﾄｻｲﾌｧｰ）	ﾛｰﾚﾙｲﾝﾃﾘｼﾞｪﾝﾄｼｽﾃﾑｽﾞ	ﾉｱ･ﾋﾞｼﾞﾈｽ	共通鍵	SXAL/MBAL		ﾌｧｲﾙ・ﾃﾞｰﾀ暗号化
SmartSafe for Notes	BIG ﾍﾞｰｽﾄ情報ｼｽﾃﾑ	ﾉｱ･ﾋﾞｼﾞﾈｽ	共通鍵	SXAL/MBAL		Lotus Notes 対応ｿﾌﾄｪｱ
Soliton IPSec	ｿﾘﾄﾝｼｽﾃﾑｽﾞ	ｿﾘﾄﾝｼｽﾃﾑｽﾞ	共通鍵	DES, TripleDES, FEAL	IPSec	暗号化ｿﾌﾄｪｱ
SSH Internet Key Exchange	SSH Communications Security	SSH Communications Security	共通鍵 公開鍵 ﾊｯｼｭ	DES(56bit), TripleDES(168bit), Blowfish(40 ～ 4467bit), CAST(80bit 以上) RSA SHA-1, MD5	X.509, IKE, ISKAMP, PKCS	鍵管理ｿﾌﾄｪｱ
Tripwire	Tripwire	東芝情報ｼｽﾃﾑ		El Gamal(128bit)、RSA 相当		不正ｱｸｾｽ検知ｿﾌﾄｪｱ
Tumbleweed IME 4.0	Tumbleweed Communications	ﾀﾝﾌﾞﾙｳｨｰﾄﾞ・ｺﾐｭﾆｹｰｼｮﾝｽﾞ	共通鍵 ﾊｯｼｭ 鍵配送	RC4 MD5,SHA-1 Deiffie-Hellman(512bit)	SSL PKI	ｾｷｭｱﾊﾟｯｹｰｼﾞ配信ｿﾌﾄｪｱ
VerSecure	Hewlett Packard	日本 HP	共通鍵 公開鍵 鍵配送	DES(56bit), TripleDES(128bit), RC2(40 ～ 128bit), RC4(40 ～ 128bit) RSA(256～2048bit) Deiffie-Hellman(512～2048bit)	IPSec	ﾊｰﾄﾞｳｪｱﾍﾞｰｽ暗号ﾌﾚｰﾑﾜｰｸ
WinSafe Lite	ｼｽﾃﾑﾆｰｽﾞ	ｼｽﾃﾑﾆｰｽﾞ	共通鍵	ｶｵｽ量子化多値暗号(56bit),DES(56bit)		ﾃﾞｰﾀ暗号化ｿﾌﾄｪｱ
あい言葉	ｼｽﾃﾑﾆｰｽﾞ	ｼｽﾃﾑﾆｰｽﾞ	共通鍵	ｶｵｽ量子化多値暗号(56bit)		IC ｶｰﾄﾞ対応ﾃﾞｰﾀ暗号化ｿﾌﾄｪｱ

暗号ﾌﾟﾛｾｯｻ	富士通	富士通	共通鍵 公開鍵	DES(56bit),TripleDES(168bit) RSA(最大 2048bit)		暗号化 PCI ﾎﾞｰﾄﾞ
暗号ﾌﾟﾛｾｯｻ	富士通	富士通	共通鍵	DES(56bit),TripleDES(168bit)		GS8000 向け暗号ﾌﾟﾛｾｯｻ
安心金庫 PRO Group Edition	ﾄﾗﾝｽｺｽﾓｽ	ﾄﾗﾝｽｺｽﾓｽ	共通鍵	TEE128(128bit), GOST, DES(56bit), TripleDES(168bit), Blowfish(128/160bit)		動的鍵共有ｱﾙｺﾞﾘｽﾞﾑ(1024bit)使用 ｿﾌﾄｪｱ
回線暗号装置	NTT ｴﾚｸﾄﾛﾆｸｽ	NTT ｴﾚｸﾄﾛﾆｸｽ	共通鍵	FEAL、DES 及び TripleDES		ﾊｰﾄﾞｳｪｱ
ｶｵｽﾘﾓｺﾝ v2.02	国際情報科学研究所	国際情報科学研究所	共通鍵	GCC ｶｵｽ暗号（320bit）		ﾒｰﾙ暗号化ﾘﾓｺﾝ ｿﾌﾄｪｱ
ｶｵｽﾘﾓｺﾝ v2.2	国際情報科学研究所	国際情報科学研究所	共通鍵	GCC ｶｵｽ暗号（320bit）	S/MIME PGP	暗号ﾘﾓｺﾝ ｿﾌﾄｪｱ
ｸﾘﾌﾟﾃｨﾎﾞｰﾄﾞ 710B	NTT ｴﾚｸﾄﾛﾆｸｽ	NTT ｴﾚｸﾄﾛﾆｸｽ	共通鍵 公開鍵	DES(56bit), TripleDES 公開鍵（最大 2048bit）	FIPS140-1 Level3	暗号ﾎﾞｰﾄﾞ
ｽﾏｰﾄｾﾃﾞｯｸ	大日本印刷	大日本印刷	共通鍵 公開鍵	DES(56bit) RSA(512/576bit)		ﾃﾞｰﾀ分割＆暗号ｼｽﾃﾑ
ｾｷｭｱｻｰﾋﾞｽﾌﾟﾗｯﾄﾌｫｰﾑ	ＮＴＴｱﾄﾞﾊﾞﾝｽﾃｸﾉﾛｼﾞ	ＮＴＴｱﾄﾞﾊﾞﾝｽﾃｸﾉﾛｼﾞ	共通鍵	FEAL, DES		認証、権限、暗号化のﾌﾟﾗｯﾄﾌｫｰﾑ
ﾉｷｱ IP ｼﾘｰｽﾞ	NOKIA	NOKIA ﾈｯﾄﾜｰﾙﾄﾞ ｲﾝﾃｯｸ KDD 東芝情報ｼｽﾃﾑ	共通鍵	DES(56bit), RC4(40bit), FWZ-1		統合型ﾌｧｲｱｳｫｰﾙ、ﾙｰﾀ
秘文/Enterprise	日立ｿﾌﾄｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ	日立ｿﾌﾄｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ	共通鍵	IDEA		ﾈｯﾄﾜｰｸ対応自動ﾌｧｲﾙ暗号ｿﾌﾄ
秘文/SAFE	日立ｿﾌﾄｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ	日立ｿﾌﾄｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ	共通鍵	IDEA		自動ﾌｧｲﾙ暗号ｿﾌﾄ
盗聴防止電話機	NTT ｴﾚｸﾄﾛﾆｸｽ	NTT ｴﾚｸﾄﾛﾆｸｽ	共通鍵	鍵長 128bit 使用		ﾊｰﾄﾞｳｪｱ

第 5 章　ファイアウォール技術

5.1　はじめに

近年のインターネットの普及に伴い、E コマース等、企業におけるインターネット利用は増加の一途を辿っており、多くの企業がインターネットへの常時接続環境を構築している。

一方、昨年 1 月に起きた中央省庁の HP 改ざん事件に代表されるような不正アクセス事件も増加しており、インターネットからの不正アクセス対策は企業にとって必須となっている。インターネットからの不正アクセスにより、機密情報の漏洩や社会的信用の失墜等、企業は様々な損害を被る可能性がある。

本章では、インターネットからの不正アクセスを防止するための代表的な技術であるファイアウォール技術について、その役割、機能等を述べるとともに、ファイアウォールによって防御可能な攻撃、防御できない攻撃を明らかにし、さらには防御できない攻撃についての対策を検討する。

5.2　ファイアウォール概要

(1) ファイアウォールの役割

ファイアウォールは、企業のプライベートネットワークとインターネットの接続点において、インターネットからの不正アクセスから企業のプライベートネットワークを保護することを主目的として利用される。

(2) ファイアウォールの分類

ファイアウォールは、中継するデータの検査レベルから以下の３タイプに分類可能である。

1)パケットフィルタリング型ファイアウォール

①概要

ネットワーク層で動作し、パケットヘッダ情報を基準にしてフィルタリングを実施する。フィルタリングには発信元･送信先 IP アドレスやポート番号に関する情報を利用する。

②利点

パケットフィルタリングはルーターの標準機能であるため、インターネット接続に使用するルーターをファイアウォールとして利用する場合、インプリメントにはほとんど費用がかからない。また、他方式と比較してパフォーマンスが良い。

③制限

パケットフィルタリング方式は、高いパフォーマンスを実現しやすい一方で、通信の“状態”を覚えておくことができないという短所がある。そのため、図５－１に示すように許可する範囲を“大きめ”に設定する必要がある。

このため、最近ではパケットフィルタリング機能と、後述するステートフルインスペクション機能を組み合わせたファイアウォール製品が数多く提供されている

図５－１　外部 HTTPを許可する場合のイメージ図

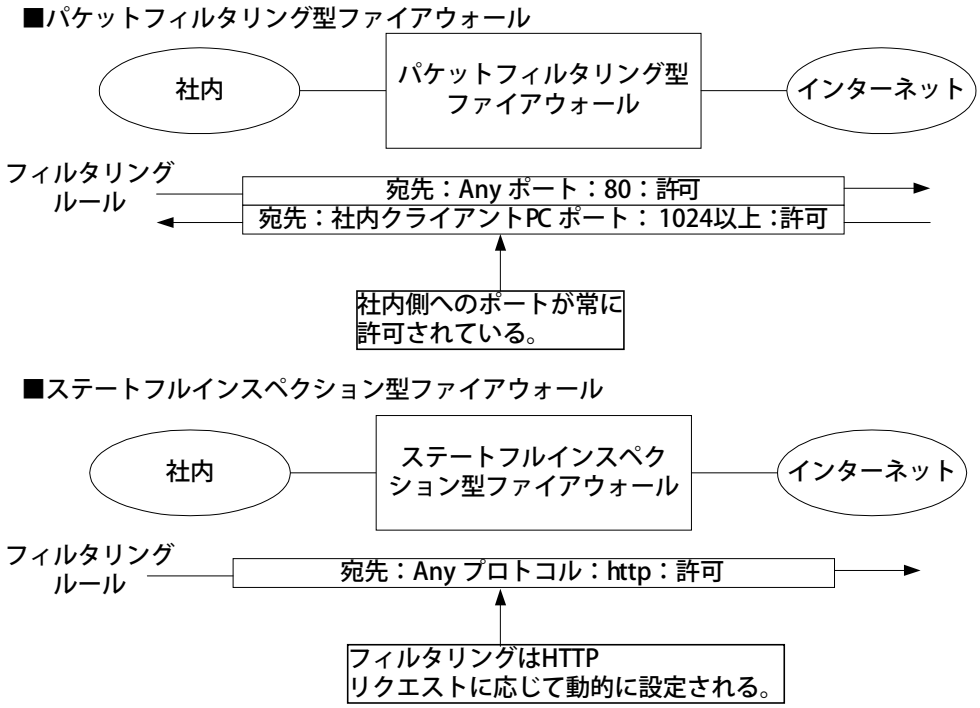


図１：外部HTTPを許可する場合のイメージ図

2)サーキットレベル型ファイアウォール

①概要

トランスポート層で動作する。代表的な方式に SOCKS がある。SOCKS では sockd というプログラムを介してクライアントとサーバー間で通信する。このとき TCP の論理セッションはクライアントとファイアウォール(SOCKS)とアプリケーションサーバーとファイアウォール(SOCKS)の 2 つが sockd によって接続する。

②利点

トランスポート層でパケットの中継を実施するため、パケットフィルタリング型ファイアウォールと違い、外部パケットが内部に流入するリスクを回避することが可能である。

③制限

複数のアプリケーションプロトコルを 1 つの仕組みで中継するため、個々のアプリケーションプロトコルで決められたコマンドごとの制限などができない。

3)アプリケーションゲートウェイ型ファイアウォール

①概要

アプリケーション層で動作し、中継するパケットのデータの中身まで、検査して中継の可否を判断する。

②利点

データの中身まで検査するため、例えば、ftp の put、get などプロトコルコマンドをチェックし、転送の方向を制限するなど詳細な制限を実施することが可能である。

③制限

パケットフィルタリング型と比較してパフォーマンスが落ちるという短所がある。

また、各アプリケーションプロトコルごとに専用プログラムが必要となる。

4)ステートフルインスペクション型ファイアウォール

①概要

ステートフルインスペクションはチェックポイントソフトウェアテクノロジーズ社によって開発された新しいファイアウォール技術である。ステートフルインスペクションは、パケットフィルタリング型、サーキットレベル型、アプリケーションゲートウェイ型のファイアウォールが持つ欠点を改良する方式である。

カーネルの中で動作するインスペクトエンジンと呼ばれるモジュールを搭載している。インスペクトエンジンは、通信やプロトコルの内容を監視、解析し、通信の状態に応じてフィルタルールを追加、削除する。

ステートフルインスペクション機能は、図５－１に示すようにパケットフィルタリング型ファイアウォールと比較すると、必要なパケットだけが通過できるため、高いセキュリティレベルを実現できる。また、カーネルの中で動作するため、アプリケーションゲートウェイ型ファイアウォールと比較して、パフォーマンスも良好である。

(3) ファイアウォールのシステム構成

1)基本構成

ファイアウォールのネットワーク構成は様々な形態が取られるが、図５－２に示すような DMZ（DeMilitarized Zone：非武装地帯）と呼ばれる第３セグメントを設け、DMZ に Web サーバー、メールサーバーなどインターネットに公開するサーバーを設置する構成が一般化してきている。

インターネットに公開するサーバーを、社内ネットワークとは独立したネットワークセグメントに設置することにより、インターネットサーバーに不正アクセスが発生した場合にも、被害が社内まで拡大することを防止できる。

図５－２　DMZを使用したファイアウォールのネットワーク構成例

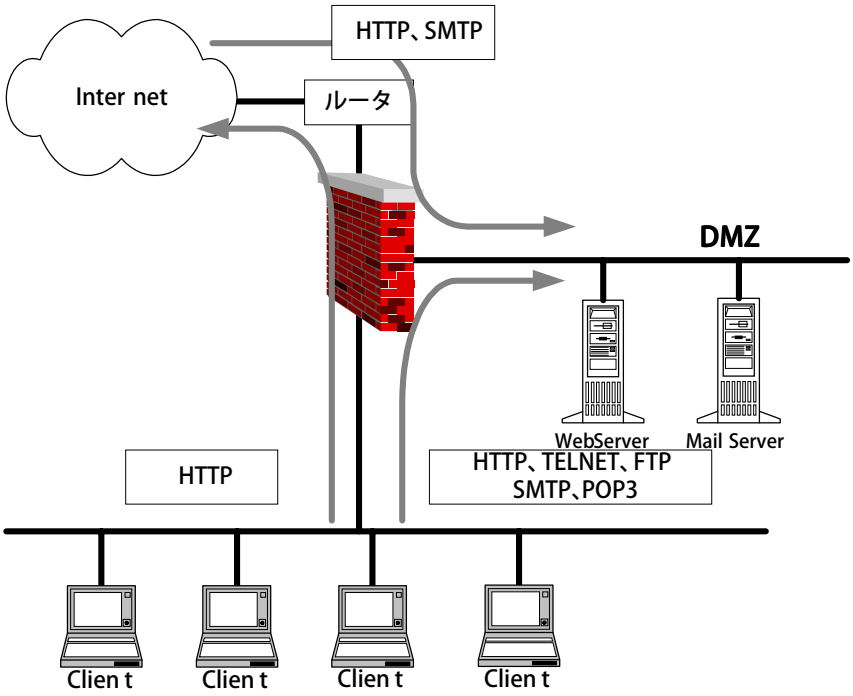


図２：ＤＭＺを使用したファイアウォールのネットワーク構成例

2)製品選択

ファイアウォールを構築する方式としては、ルーターを利用した方式なども考えられるが、専用のファイアウォールソフトウエアを利用する方式が一般的のようである。

以前は UNIX や NT などの汎用機にファイアウォールソフトウエアを導入するのが一般的であったが、最近では、主として中小規模のネットワークを対象として、専用のハードウエアとファイアウォールソフトウエアをセットにした一体型のファイアウォール製品が普及してきている。これらの製品は、汎用機にファイアウォールソフトウエアを導入する方式と比較して、設定、管理が容易であるという特長がある。

製品選択にあたっては、ファイアウォール機能以外の VPN 機能やユーザー認証機能の有無等の要求仕様に合った製品選択をすることはもちろんのこと、それ以外にも販売元から十分なサポートを得られるか、製品のシェアはどの程度かといった内容も考慮する必要があると思われる。

また、最近ではインターネット接続サービスとファイアウォール機能をセットで提供する ISP も多数存在するので、自社での運用が難しい場合は、このような方式を選択する方法もある。

表５－１　ファイアウォール製品の一例

製品名	開発元	方式				その他の機能		対応OS	価格
		PF *1	CL *2	AG *3	SI＋PF *4	VPN	ユーザ認証		
Firewall-1	チェックポイントソフトウェアテクノロジーズ（イスラエル）				○	FW-FW *5 FW-CL *6	S/Key SecureID RADIUS	WindowsNT Solaris HP-UX 独自 OS(Nokia)	25 ノード版 49 万円～
NetGUARDIAN	ネットガードド（イスラエル）	○				FW-FW	S/Key	WindowsNT	25 ユーザ版 28 万円～
Goahnet /Privatenet SVII	日本電気	○	○	○		FW-FW FW-CL	独自	UX/4800	20 接続版 138 万円～ (H/W 込)
Gauntlet	ネットワークアソシエイツ(米)	○		○		FW-FW FW-CL	RADIUS	NT、Solaris HP-UX	無制限版 198 万～
Raptor Firewall	アクセントテクノロジーズ(米)	○		○		FW-FW FW-CL	固定パスワード NT ドメイン TACACS+ Radius S/KEY SecurID	NT、Solaris HP-UX	25 ユーザ版 37,5 万円～
Fire les s	コンテック				○	FW-FW	×	独自 OS	ユーザ数無制限 38 万～
Fort Knox	アルカテル（仏）	○		○		FW-FW FW-CL	SecureI D	独自 OS	1デバイス 194,000 円から
NetScreeen	ネットスクリーンテクノロジーズ (米)				○	FW-FW FW-CL	独自 RADIUS	独自 OS	10ユーザ版 オープン
SonicWall	ソニックウォール(米)				○	FW-FW FW-CL	RADIUS	独自 OS	10ユーザ 14万円～
GNATBOX	グローバルテクノロジアソシエイツ(米)				○	FW-FW		独自 OS	ハード一体型 40万円
WatchGuard	ウォッチガードテクノロジーズ (米)			○	○	FW-FW FW-CL	独自 RADIUS NTドメイン	独自 OS	無制限版 87,8 万円～

＊順不同
*1 PF：パケットフィルタリング型
*2 CL：サーキットレベル型
*3 AG：アプリケーションゲートウェイ型
*4 PF＋SI：ステートフルインスペクションパケットフィルタリング型
*5 FW-FW：拠点間 VPN
*6 FW-CL：クライアント PCからのリモートアクセス

5.3　ファイアウォール以外の対策

(1) ファイアウォールで防御できない攻撃

ファイアウォールは、許可されていない発信元・送信先への通信の遮断や、許可されていないプロトコルの通信の遮断が可能である。しかしながら、インターネットに公開しているサービス（例、Web サーバー、メール、DNS など）は、ファイアウォールで通信を許可しているため、これらのサービスのセキュリティホールを利用した攻撃や、設定ミスを利用した攻撃を防ぐことはできない。

ファイアウォールでは防御できない攻撃の例を挙げると、

①各種サーバーのセキュリティホールを利用した攻撃による管理者権限の奪取
②各種サーバーのセキュリティホールを利用した DOS 攻撃
③各種サーバーのセキュリティホールを利用した攻撃による情報漏洩
④セキュリティホールのないサーバーへの DOS（DDOS）攻撃
⑤セキュリティホール、設定ミスのあるメールサーバーをスパムメールの踏み台に利用
⑥セキュリティホール、設定ミスのあるサーバーを乗っ取り、DDOS 攻撃の踏み台に利用

①～④は自社が被害に及ぶが、⑤、⑥では自社を踏み台にして他社サイトを攻撃することになるため、後々、攻撃対象のサイトから訴えられる可能性がある。

(2) ファイアウォールで防御できない攻撃の対策

ファイアウォールで防御できない攻撃を防止するためには、自社のサーバーの各ソフトウエアを正しく設定し、かつ、セキュリティホールのない安全な状態に維持する必要がある。そのためには、

・サーバーのハードウエアベンダー、ソフトウエアベンダーから継続的にセキュリティ情報を入手する
・インターネット上のセキュリティ関連サイトから継続的にセキュリティ情報を入手する。
・インターネット上のメール不正中継チェックサイトを利用して設定ミスの有無を確認する

等を利用して継続的に情報収集し、問題が発生した場合に速やかに対応する必要がある。

以下にインターネット上のセキュリティに関する情報源として参考となるサイトを列挙する。

○インターネット上のセキュリティ関連情報サイト

CERT/CC：http://www.cert.org/
Security Focus：http://www.securityfocus.com/
Microsoft 社のセキュリティ情報サイト：http://microsoft.com/japan/technet/security/

○メールサーバーの不正中継チェックサイト

Open Relay Behaviour-modification System ホームページ：http://www.orbs.org/
Mail Abuse Prevention System ホームページ：http://maps.vix.com/

(3) 不正アクセスの常時監視

サーバーをセキュアにすることにより、サーバーのセキュリティホールを利用した攻撃まで防御可能となる。さらに侵入検知システムを利用することにより、常時監視が可能となる。侵入検知システムに関する詳細は第６章で述べる。

●参考文献

・UNIX マガジン 2001 年 1 月 p12～21「いつでも使えるインターネット 個人の常時接続を考える（7）」白崎博生
・リクルート キーマン‘S ネット http://www.keyman.or.jp/
・日経インターネットテクノロジー 2000 年 3 月号 p94～101
・日経システムプロバイダー2000.2.4 p 52～54
・Firewall Defenders (電脳火消隊)ホームページ：http://www.firewall.gr.jp/
・Open Relay Behaviour-modification System ホームページ：http://www.orbs.org/
・Mail Abuse Prevention System ホームページ：http://maps.vix.com/
・有限会社長崎ネットワークサービスホームページ：http://www.nanet.co.jp/

第６章　不正アクセス監視技術

６．１　侵入検知システム

(1) 必要とされる背景

インターネットなどの外部ネットワークと接続された情報システムのセキュリティを守るための対策としてはファイアウォールの設置が一般的である。

しかし、不正アクセスの手口は日々巧妙化しており、加えて、さまざまなツールが作成され流通していることから、ファイアウォールを設置していれば不正アクセス対策は万全ということにはならない。外部からのアクセス状況を常に監視し危険な兆候があった場合にアクセスを遮断するなど、迅速な対応がとれる措置が必要である。

一方、不正アクセスの８割が内部犯行といわれる社会情勢においては、社内のクライアントから業務サーバーへのアクセス状況についても監視し、不正アクセスの兆候を把握する措置および万が一問題が発生した場合に侵入者の特定と証拠保全を行える措置も必要である。

これらの問題に対する万全な対応策は現時点では存在しないが、侵入検知システムにより概ね対処することが可能である。

(2) システムの概要

侵入検知システム（IDS：Intrusion Detection System）は、ネットワークやサーバーへのアクセス状況の監視、侵入抑止、侵入者特定、証拠保全を行うもので、情報ネットワークのセキュリティ侵害を防止するための技術として昨今注目されているものである。

システムのイメージとしては、防犯カメラのようなもので設置された場所の状況を常時監視する。主な機能は次のとおりである。

①アクセスの記録を保存するとともに監視モニターに表示する。

②不正アクセスあるいはその兆候に対してコネクションの切断や通信経路の遮断を行い、侵入を未然に抑止する。また、管理者に対し自動的に通報する。

(3) ツールの種類

侵入検知システムで使用するツールは大きく２種類に分類され、ネットワーク上を流れるパケットを監視する「ネットワーク監視型」と、サーバー上でアクセス者の挙動を監視する「ホスト監視型」がある。

(4) ネットワーク監視型侵入検知システム

1) システム構成

システムは、パケットを収集する「センサー」と、センサーから情報を受け取って表示・分析など集中管理を行う「コンソール」から構成される。

センサーは２枚の NIC を装備し、片方の NIC を監視対象のネットワークに「プロミスキャスト・モード（すべてのパケットを収集することから無差別モードともいう）」という設定で接続する。また、センサー自体が攻撃対象になるのを防ぐため IP アドレスを設定せず、一切送信を行わない「ステルス・モード」という設定を併せて行う。もう一方の NIC はコンソールとの通信を行うために別ネットワークに接続する。

2) 不 正アクセスの判断ロジック

収集したパケットを攻撃手法のデータベースと許可する行動などの規則（ルール）を組み合わせた「ポリシー」とのパターン・マッチングにかけ、不正アクセスか否かの判断が行われる。

パターン・マッチングの結果不正アクセスと判断した場合、管理者への自動通報や TCP コネクションの強制切断、ファイアウォールやルーターと連携した通信経路の遮断などの防御処理が行われる。

3) 特 徴

クラッカーなどが不正アクセスの前段階として利用するポートスキャンや DoS 攻撃（サービス不能攻撃）などを発見するのに向いているが、クラッカーが事前に何らかの方法で ID/パスワードを入手して、正規のユーザーになりすまして行う行為に対しては弱い。

(5) ホスト監視型侵入検知システム

1) シ ステム構成

システムは、サーバーへのアクセス状況を監視する「エージェント」と、エージェントから情報を受け取って表示・分析など集中的に管理を行う「コンソール」からなる。

エージェントは、監視対象のサーバーに直接インストールする。

2) 不 正アクセスの判断ロジック

サーバーのログを監視して情報を収集し、攻撃手法のデータベースとユーザーのファイル・アクセス権限および許可する行動などの規則（ルール）を組み合わせた「ポリシー」とのパターン・マッチングで比較して不正アクセスを検知する。

パターン・マッチングの結果不正アクセスと判断した場合には、管理者への自動通報や TCP コネクションの強制切断などの防御処理が行われる。

3) 特 徴

正規のユーザーであっても不審な行動をとれば不正アクセスとして発見することができるが、ポートスキャンや DoS 攻撃（サービス不能攻撃）など、パケット・レベルの不正アクセスには基本的には対処できない。

(6) 製品選定のポイント

選定にあたっては、いかに多くの種類の侵入手法を確実に検出できるか、設定の容易性、ログの表示やレポートの作成機能の充実度合い、日本語対応などを考慮すべきである。

なお、ネットワーク監視型の場合、ネットワーク構成（トラフィックが多いネットワーク、二重化されたネットワーク等）に応じてセンサー設置箇所の考慮が必要である。

ホスト監視型の場合は、エージェントをインストールすることによりサーバー上で稼働している自社開発のアプリケーションなどに対する影響の有無について確認する必要がある。

(7) 主な侵入検知システム用ツール

表 6－1

(8) 不正アクセスの手口と侵入検知システムでの対応

表 6－2（別表）　参照。

別表６－１　主な侵入検知システム用ツール

製品名	開発／販売	監視方式	対応ＯＳ	検出項目数	ﾚﾎﾟｰﾄ	他機器との連携	価格
CyberCop Monitor	ﾈｯﾄﾜｰｸｱｿｼｴｲﾂ	ホスト監視型	WindowsNT Solaris HP-UX	168	英語	可	26 ﾃﾞﾊﾞｲｽ 254,800 円～
Intruder Alert	日新電機	ホスト監視型	WindowsNT HP-UX NetWare など	約 300	英語	不可	ｺﾝｿｰﾙ 500,000 円 ｴｰｼﾞｪﾝﾄ 20,000 円
Kane Security Monitor	ｾｷｭﾘﾃｨﾀﾞｲﾅﾐｸｽ	ホスト監視型	WindowsNT	約 20	日本語	不可	1 ｻｰﾋﾞｽﾗｲｾﾝｽ 298,000 円～
NetProwler	日新電機	ﾈｯﾄﾜｰｸ監視型	WindowsNT	158	英語	可 ﾌｧｲｱｳｫｰﾙ	1,100,000～
NetRanger	日本 Cisco Systems	ﾈｯﾄﾜｰｸ監視型	Solaris	約 200	英語	可 ﾙｰﾀ	4,736,000 円～
RealSecure Network Sensor	ISS	ﾈｯﾄﾜｰｸ監視型	WindowsNT Solaris Linux	338	日本語	可 ﾌｧｲｱｳｫｰﾙ ﾙｰﾀ	1 ﾃﾞﾊﾞｲｽ 1,079,000 円～
RealSecure OS Sensor	ISS	ホスト監視型	WindowsNT Solaris	186	日本語	可 ﾌｧｲｱｳｫｰﾙ ﾙｰﾀ	1 ﾃﾞﾊﾞｲｽ 194,000 円～
SessionWall-3	Computer Associates	ﾈｯﾄﾜｰｸ監視型	WindowsNT	117	日本語	可 ﾌｧｲｱｳｫｰﾙ ﾙｰﾀ	25 ﾕｰｻﾞ版が 390,000 円～

※品名（アルファベット）順

別表６－２　不正アクセスの手口と侵入検知システムでの対応

不正アクセスの手口	不正アクセスの内容	攻撃元と危険度		侵入検知システムでの対応
		外部	内部	
①ポートスキャン	ツールなどを使用し、サーバに対して空きポートや稼働しているサービスの検索を行う。	高	中	ﾈｯﾄﾜｰｸ監視型：○ ホスト監視型：×
②DoS 攻撃	不正なパケットなどをサーバに対し送り付け、ダウンさせる。	高	中	ﾈｯﾄﾜｰｸ監視型：○ ホスト監視型：×
③メール爆弾	大量のメールを送り付け、ダウンさせる。	高	低	×
④踏み台	メール爆弾を送信するために、他のメールサーバを不正に使用する。	高	低	×
⑤セキュリティホールからの不正侵入	セキュリティホールを狙い、バッファオーバーフローなどを行いサーバへ侵入する。	高	低	○
⑥なりすましによる不正侵入	正規ユーザの ID やパスワードを盗み、なりすましサーバへ侵入する。	低	高	ﾈｯﾄﾜｰｸ監視型：× ホスト監視型：○
⑦データの改ざん	サーバへ侵入後、データの改ざんや消去を行う。	中	中	ﾈｯﾄﾜｰｸ監視型：× ホスト監視型：○
⑧バックドアやトロイの木馬	サーバへ侵入後、再度侵入したり遠隔操作を行うための不正なプログラムを仕掛ける。	中	中	○
⑨盗聴	ネットワーク上を流れるパケット（パスワード、メッセージデータなど）を盗聴するプログラムを仕掛ける。	中	高	×

③は現時点では防ぐ手段は存在しない。
④はメールサーバに適切な処置を施すことで対応可。
⑨は不許可の情報機器の LAN接続／プログラムの不正インストールに対する管理強化、対盗聴ツールによる細やかな調査等の対応が必要。

６．２　セキュリティ診断ツール

(1) 必要とされる背景

不正アクセスはシステムの潜在的なセキュリティホールや設定上の不備をついて行われることが多い。

システム構築でサーバーやネットワーク機器を設定する際、セキュリティ面に十分注意しても意図しない設定の不備や、潜在的なセキュリティホールまで人的に対処するには自ずと限界がある。

セキュリティ診断ツールを使用してシステムの脆弱性の検査を行い、発見された問題点に対する対策を実施することで、よりセキュリティの高いシステム構築が可能となる。

(2) ツールの概要

セキュリティ診断ツールは、サーバーやネットワーク機器に対するセキュリティホールを調査するためのもので、診断対象のサーバーやネットワーク機器に対して擬似的な攻撃を仕掛けて安全性をチェックする。

(3) ツールの種類

セキュリティ診断ツールは大きく２種類に分類され、ネットワーク経由で診断対象のサーバーやネットワーク機器を診断する「外部診断型」と、診断対象のサーバーやネットワーク機器上で稼動させる「内部診断型」がある。

(4) 外部診断型ツール

1) 検 査方法

診断用ツールをインストールした機器をインターネットあるいは社内 LAN に接続し、診断するサーバーやネットワーク機器に対し疑似攻撃を行い弱点を発見する。

検査内容としては、ネットワークからの不正なアクセスや攻撃が可能なセキュリティホールの有無、稼働している Sendmail、FTP、DNS などのアプリケーションが持つ問題点、ファイアウォール、ルーター、Web サーバーの問題点、OS 固有の問題点などがあり、診断用ツールがもつ検査用データベースに設定されている。

2) 特 徴

ネットワークに接続されたサーバーやネットワーク機器の潜在的な問題点を、ネットワークを介して外部からの不正侵入者と同じ視点で客観的に検査することが可能である。

レジストリやパーミッションなど設定上の問題点の洗い出しは内部診断型には及ばない。

(5) 内部診断型ツール

1) 検 査方法

診断するサーバーに診断用ツールをインストールし、潜在的な問題点を内部から検査す

る。

検査内容としては、各ファイルのパーミッション設定、パッチの適用有無、ソフトウエアのバージョンおよびコンフィグレーション、使用可能なネットワークサービス、推測可能なユーザーパスワードの有無などがあり、診断用ツールがもつ検査用データベースに設定されている。

また、前回の検査結果と比較を行い、管理者が認知していないパーミッションの変更、アカウントの追加など、不正アクセスの痕跡の洗い出しも行う。

2) 特 徴

OS における弱点を見つけだすもので、外部診断型では発見しにくいレジストリやパーミッションなど設定上の問題点などを洗い出すことが可能である。

(6) 製品選定のポイント

選定にあたっては、いかに多くの種類の潜在的な問題点を検出できるか、対象になる機器の種類や設定の容易性、発見された項目のレポートの作成機能の充実度合いや対応策の表現の難易度、日本語対応などを考慮すべきである。

なお、内部診断型の場合、診断ツールをインストールすることによりサーバー上で稼働している自社開発のアプリケーションなどに対する影響の有無についても確認する必要がある。

(7) 主な診断ツール

表６－３参照。

表６－３　主な診断ツール

製品名	販売	診断方式	対応ＯＳ	診断項目数	価格
CyberCop Scanner	ﾈｯﾄﾜｰｸｱｿｼｴｲﾂ	外部診断型	WindowsNT Linux	540	26ﾉｰﾄﾞ 220,000円から
Internet Scanner	ISS	外部診断型	WindowsNT Solaris Linux	597	10ﾃﾞﾊﾞｲｽ 250,000円から
NetRecon	日新電機	外部診断型	WindowsNT	約300	600,000円から
NetSonar	日本Cisco Systems	外部診断型	WindowsNT	約300	760,000円から
System Scanner	ISS	内部診断型	WindowsNT Solaris HP-UX Linuxなど	約200	1ﾃﾞﾊﾞｲｽ 150,000円から

※品名（アルファベット）順